UE
Proiect

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr.

din 2026

Chișinău

cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații

---

În temeiul art. 6 alin. (2), (6) și (7), art. 19 alin. (8), art. 22 alin. (2), art. 42 alin. (4) și art. 56 alin. (2) din Legea nr. 209/2026 privind cooperarea polițienească internațională (Monitorul Oficial al Republicii Moldova, 2026, nr. 486 - 489, art. 505), Guvernul HOTĂRĂȘTE:

Prezenta Hotărâre:

- transpune parțial Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024 privind căutarea și schimbul automatizat de date în scopul cooperării polițienești, și de modificare a Deciziilor 2008/615/JAI și 2008/616/JAI ale Consiliului și a Regulamentelor (UE) 2018/1726, (UE) 2019/817 și (UE) 2019/818 ale Parlamentului European și ale Consiliului (Regulamentul Prüm II), publicat în Jurnalul Oficial al Uniunii Europene L 2024/982 din 5 aprilie 2024, CELEX: 32024R0982;

- transpune parțial Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere, publicată în Jurnalul Oficial al Uniunii Europene, L 210 din 6 august 2008, așa cum a fost modificată ultima oară prin Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024, CELEX: 32008D0615;

- transpune parțial Decizia 2008/616/JAI a Consiliului din 23 iunie 2008 privind punerea în aplicare a Deciziei 2008/615/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere, publicată în Jurnalul Oficial al Uniunii Europene, L 210/12 din 6 august 2008, așa cum a fost modificată ultima oară prin Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024, CELEX: 02008D0616-20240425;

- transpune parțial Directiva (UE) 2023/977 a Parlamentului European și a Consiliului din 10 mai 2023 privind schimbul de informații dintre autoritățile de aplicare a legii ale statelor membre și de abrogare a Deciziei-cadru 2006/960/JAI a

Consiliului, publicată în Jurnalul Oficial al Uniunii Europene, L 134/1 din 22 mai 2023, CELEX: 32023L0977;

- transpune parțial Decizia 2004/919/CE din 22 decembrie 2004 privind combaterea criminalității referitoare la vehicule și având implicații transfrontaliere, publicată în Jurnalul Oficial al Uniunii Europene, L 389/28 din 30 decembrie 2004, CELEX: 320004D0919.

1. Se desemnează următoarele autorități în calitate de Puncte Naționale de Contact, pe domenii de competență, care au obligația de a asigura accesul Punctului Unic de Contact la datele de referință și de a furniza, în limitele competenței funcționale, informațiile necesare realizării schimburilor de date:

1.1. ***Centrul tehnico-criminalistic și expertize judiciare al Inspectoratului General al Poliției*** – pentru domeniile de profiluri ADN, date dactiloscopice și imagini faciale, în partea ce ține de examinarea, verificarea și validarea de specialitate a concordanțelor;

1.2. ***Serviciul Tehnologii Informaționale, autoritate administrativă în subordinea MAI*** – în calitate de deținător și administrator tehnic al sistemelor informaționale de stat din domeniul afacerilor interne care conțin evidențe cu caracter criminal, contravențional, datele nominale privind persoanele urmărite, dispărute fără veste sau implicate în activități infracționale, în condițiile și limitele prevăzute la art. 20-22 din Legea nr. 209/2026 privind cooperarea polițienească internațională, date referitoare la vehiculele anunțate în căutare, precum și piesele componente ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, precum și pentru datele dactiloscopice (în partea asigurării funcționării Sistemului informațional automatizat „Registrul de stat dactiloscopic” și a comunicațiilor aferente schimbului de date dactiloscopice);

1.3. ***Inspectoratul General de Carabinieri, autoritate administrativă în subordinea MAI*** – pentru domeniul evenimentelor majore cu dimensiune transfrontalieră;

1.4. ***Agenția Servicii Publice*** – pentru domeniul de date privind mijloacele de transport, date privind documentele de călătorie, inclusiv a celor declarate false, furate sau pierdute, precum și date privind permisele de conducere;

1.5. ***Serviciul de Informații și Securitate*** – pentru domeniul furnizării informațiilor necesare prevenirii infracțiunilor cu caracter terorist, în regim de informații indirect accesibile, în condițiile, limitele și conform procedurilor prevăzute de legislația națională.

1.6. ***Serviciul Tehnologia Informației și Securitate Cibernetică*** – în calitate de punct național de conectare la domeniul local la rețeaua de comunicații securizată a Uniunii Europene TESTA, responsabil de asigurarea conectivității, funcționării, disponibilității și securității canalului național de comunicații utilizat pentru schimbul de date.

2. Se aprobă:

2.1. Regulamentul privind organizarea și funcționarea Punctului Unic de Contact în scopul schimbului de date și informații, conform anexei nr. 1;

2.2. Regulamentul privind organizarea și funcționarea Punctelor Naționale de Contact în scopul schimbului de date și informații, conform anexei nr. 2.

3. Autoritățile competente de aplicare a legii care exercită atribuții în domeniul activității speciale de investigații, organele de urmărire penală, precum și alte autorități naționale relevante care dețin informații relevante pentru prevenirea, depistarea sau investigarea infracțiunilor, inclusiv informații indirect accesibile, au obligația de a coopera activ cu Punctul Unic de Contact, de a acorda suportul necesar și de a furniza, fără întârzieri nejustificate, datele și informațiile solicitate în vederea asigurării îndeplinirii sarcinilor Punctului Unic de Contact prevăzute de prezenta hotărâre.

4. Controlul asupra executării prezentei hotărâri se pune în sarcina autorităților din cadrul cărora au fost desemnate Punctul Unic de Contact și Punctele Naționale de Contact, conform domeniilor de competență stabilite.

5. Prezenta hotărâre intră în vigoare la data intrării în vigoare a Legii nr. 209/2026 privind cooperarea polițienească internațională.

6. Prevederile referitoare la interconectarea tehnică și schimbul automatizat de date prin infrastructurile Uniunii Europene (Router-ul UE, EPRIS, EUCARIS, ESP, CIR, CRRS, SIS/SIRENE, SIENA, TESTA), precum și cele vizând cooperarea operațională și raportarea statistică către organismele Uniunii Europene, se vor pune în aplicare pe măsura asigurării condițiilor tehnice și juridice necesare, după obținerea de către Republica Moldova a dreptului de acces la mecanismele respective în temeiul tratatelor internaționale sau de la data aderării la Uniunea Europeană, după caz.

7. Până la asigurarea condițiilor menționate supra, schimbul de date și informații se realizează prin utilizarea canalelor de cooperare internațională deja disponibile (Interpol, SELEC, acorduri bilaterale), procedurile de triaj și validare manuală prevăzute în anexele nr. 1 și nr. 2 la prezenta Hotărâre fiind aplicate în măsura compatibilității cu aceste sisteme existente.

8. Interoperabilitatea tehnică pe segmentul național, realizată prin platforma guvernamentală MConnect și prin Sistemul electronic unic de gestionare a cazurilor, se pune în aplicare de la data intrării în vigoare a prezentei hotărâri, în scopul asigurării pregătirii infrastructurii interne pentru conectarea ulterioară la sistemele Uniunii Europene.

Prim-ministru **Vasile Tofan**

Contrasemnează:

Ministrul afacerilor interne Daniella Misail-Nichitin

Anexa nr. 1 la Hotărârea Guvernului
nr. _____ /2026

REGULAMENTUL
privind organizarea și funcționarea Punctului Unic de Contact în scopul schimbului de date și informații

I. DISPOZIȚII GENERALE

1. Regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații *(în continuarea – Regulament)* stabilește cadrul normativ pentru organizarea, funcționarea și atribuțiile Punctului Unic de Contact (*în continuare – PUC*), precum și procedurile operaționale pentru schimbul de date biometrice (profiluri ADN, date dactiloscopice și imagini faciale); date referitoare la vehicule, inclusiv autovehiculele anunțate în căutare, precum și piesele componente ale acestora consemnate cu număr de identificare urmărite internațional sau fiind obiecte ale faptelor ilegale; date privind documentele de călătorie, vizele, titlurile de valoare și permisele de conducere, inclusiv cele declarate false, furate sau pierdute; informații privind criminalitatea economică și financiară; evidențe ale poliției, inclusiv datele nominale privind persoanele urmărite, dispărute fără veste, aflate în vizorul autorităților de aplicare a legii sau implicate în activități infracționale; datele biometrice și antropometrice necesare identificării persoanelor dispărute fără veste, a cadavrelor și a părților de cadavru; datele care nu privesc persoanele și informațiile operative; datele cu caracter personal prelucrate în contextul evenimentelor majore cu dimensiune transfrontalieră și al prevenirii și combaterii infracțiunilor cu caracter terorist, precum și alte date și informații prevăzute la art. 2 alin. (4) din Legea nr. 209/2026 privind cooperarea polițienească internațională (*în continuare – Lege*).

2. Scopul prezentului Regulament este intensificarea cooperării polițienești internaționale pentru prevenirea, depistarea și investigarea infracțiunilor, precum și facilitarea căutării persoanelor dispărute fără veste și identificarea cadavrelor sau părților acestora.

Prevederile prezentului Regulament nu se aplică schimburilor de informații reglementate în mod specific de alte acte normative speciale și nu aduc atingere dreptului autorităților competente de a aplica sau încheia acorduri ori aranjamente bilaterale sau multilaterale de cooperare polițienească, în măsura în care acestea facilitează suplimentar schimbul de informații.

Schimbul de date și informații reglementat de prezentul Regulament nu instituie în sarcina autorităților naționale nicio obligație de a obține informații prin aplicarea măsurilor coercitive.

3. PUC își desfășoară activitatea în conformitate cu Legea și tratatele internaționale la care Republica Moldova este parte.

4. PUC exercită funcțiile de punct unic de contact pentru cooperarea polițienească internațională, fiind responsabil de coordonarea și gestionarea centralizată a schimbului internațional de date și informații.

5. În sensul prezentului Regulament se utilizează noțiunile definite în Lege, precum și următoarele noțiuni:

5.1. *Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Domeniul Libertății, Securității și Justiției (în continuare – eu-LISA, acronim pentru European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice)* – agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Domeniul Libertății, Securității și Justiției, responsabilă pentru administrarea tehnică și securizarea sistemelor informatice centralizate în domeniul afacerilor interne, asigurând schimbul de informații între autoritățile de aplicare a legii și de gestionare a frontierelor;

5.2. *autoritate de aplicare a legii desemnată* – orice autoritate competentă de aplicare a legii, în sensul legii, care este abilitată să transmită cereri de informații către punctele de contact unice ale statelor membre ale Uniunii Europene sau ale altor state, ori să furnizeze informații în temeiul unor astfel de cereri, conform procedurilor stabilite de prezentul Regulament;

5.3. *candidat* – setul de date de referință biometrice sau alfanumerice stocat în bazele de date ale statului solicitat, identificat în urma unei interogări automatizate ca având un grad de similitudine sau concordanță cu datele utilizate la căutare, supus procedurii de verificare și confirmare manuală;

5.4. *Centrul de răspuns la incidente cibernetice pentru instituțiile, organele și agențiile Uniunii Europene (în continuare – CERT-UE, acronim pentru Computer Emergency Response Team for the European Union institutions, bodies and agencies)* – centrul de răspuns la incidente cibernetice responsabil de protejarea infrastructurilor tehnologiei informației și comunicațiilor al instituțiilor, organelor și agențiilor Uniunii Europene, recunoscut ca echipă de sprijin operațional în domeniul securității informaționale la nivelul UE;

5.5. *Depozitul comun de date de identitate (în continuare – CIR, acronim pentru Common Identity Repository)* – depozitul centralizat de date de identitate care permite interogarea simultană a sistemelor informatice ale UE (EES, VIS, ETIAS, Eurodac) pentru identificarea persoanelor și prevenirea utilizării de identități multiple;

5.6. *Depozitul comun de raportare și statistici (în continuare – CRRS, acronim pentru Common Repository for Reporting and Statistics)* – depozitul centralizat de raportare și statistici care permite generarea rapoartelor agregate și anonime privind funcționarea și utilizarea sistemelor informatice ale Uniunii Europene, în scopul analizei operaționale și al monitorizării performanței serviciilor de interoperabilitate;

5.7. *Formatul universal pentru mesaje (în continuare – UMF, acronim pentru Universal Message Format)* – standard pentru formatul universal pentru mesaje utilizat pentru schimbul structurat de informații;

5.8. *incident de securitate cibernetică* – orice eveniment care are sau poate avea un impact asupra securității Router-ului ori a sistemului EPRIS sau care periclitează disponibilitatea, integritatea și confidențialitatea datelor prelucrate prin intermediul acestora, incluzând incidentele cibernetice semnificative, astfel cum sunt definite în Legea nr. 48/2023 privind securitatea cibernetică, ce afectează componentele naționale ale acestor sisteme;

5.9. *informații disponibile* – informații direct accesibile și informații indirect accesibile;

5.10. *informații direct accesibile* – acele informații pe care personalul PUC le poate interoga și extrage singur, în timp real, prin interfețele la care are acces autorizat (ex: Registrul de stat al populației, registrele de evidență ale poliției prin EPRIS, EUCARIS sau Sistemul de Informații Schengen);

5.11. *informații indirect accesibile* – datele care nu se află în sistemele interconectate ale PUC și necesită o solicitare către alte autorități care exercită atribuții în domeniul activității speciale de investigații, precum și către alte autorități naționale relevante sau sectorul privat, fără dispunerea aplicării măsurilor coercitive, conform dreptului național, și fără a impune autorităților respective nicio obligație de stocare a informațiilor cu unicul scop de a le furniza punctelor de contact unice sau autorităților de aplicare a legii din alte state membre ale Uniunii Europene sau alte state;

5.12. *infrastructură de comunicații securizată* – ansamblul de componente tehnice, echipamente și servicii de comunicații, inclusiv rețeaua TESTA, care asigură transportul securizat al datelor între nodul național și infrastructurile Uniunii Europene, administrată la nivel național de Serviciul Tehnologia Informației și Securitate Cibernetică (*în continuare – STISC*) în calitate de punct național de conectare;

5.13. *marcarea datelor* – procedura tehnică de aplicare a unui indicator specific (marcaj) asupra datelor cu caracter personal stocate, care poate avea ca scop fie catalogarea acestora, fie blocarea acestora, în vederea gestionării fluxurilor informaționale și informării partenerilor internaționali cu privire la statutul datelor în cadrul schimbului;

5.14. *notă* – marcajul sau indicatorul tehnic aplicat în baza de date națională asupra unui profil ADN sau asupra altor date de referință, care atestă obținerea unei concordanțe (hit) în urma unei căutări ori comparări inițiate de un alt stat membru sau de Europol, în vederea gestionării fluxului operațional și a validării ulterioare;

5.15. *Portalul european de căutare (în continuare – ESP, acronim pentru European Search Portal)* – o componentă tehnică de interoperabilitate care permite interogarea simultană și rapidă a sistemelor informatice centrale, furnizând rezultate imediate utilizatorului autorizat, fără a stoca sau a procesa datele în mod permanent;

5.16. *Servicii transeuropene securizate de telematică între administrații (în continuare – TESTA, acronim pentru Secure Trans European Services for Telematics between Administrations)* – rețea securizată de comunicații, de tip privat IP-based, utilizată la nivelul Uniunii Europene pentru schimbul de date și informații între autorități și sisteme autorizate.

6. Până la obținerea accesului deplin la infrastructurile centrale ale Uniunii Europene menționate în prezentul Regulament, schimbul de date și informații se va realiza prin utilizarea canalelor de cooperare internațională deja disponibile (Interpol, SELEC, acorduri bilaterale), cu respectarea procedurilor de triaj și validare prevăzute în prezentul Regulament, în măsura în care acestea sunt compatibile cu sistemele utilizate.

II. STRUCTURA ȘI MODUL DE ORGANIZARE ȘI FUNCȚIONARE AL PUC

Secțiunea 1
Principiile de activitate ale PUC

7. PUC își desfășoară activitatea în conformitate cu următoarele principii generale stabilite pentru activitatea Poliției:

7.1. *legalitatea, respectarea dreptului internațional și a tratatelor internaționale la care Republica Moldova este parte* - activitatea se desfășoară strict conform legii și tratatelor internaționale la care Republica Moldova este parte, fără a afecta suveranitatea sau securitatea națională;

7.2. *supremația legii, respectarea drepturilor și libertăților fundamentale ale omului* - schimbul de informații este limitat la prevenirea și investigarea infracțiunilor, respectând strict necesitatea, proporționalitatea și protecția datelor cu caracter personale;

7.3. *cooperării practice* – PUC încurajează și facilitează cooperarea practică permanentă cu autoritățile de aplicare a legii desemnate și cu Punctele Naționale de Contact. Acest principiu guvernează întreaga activitate operativă a PUC, asigurând asistența reciprocă, clarificarea procedurilor de lucru și promovarea celor mai bune practici în utilizarea canalelor securizate de comunicare, pentru a garanta un schimb de informații eficient și rapid;

7.4. *imparțialitatea și nediscriminarea persoanelor* - procedurile sunt aplicate uniform și echitabil, fără părtinire, vizând exclusiv scopuri penale bine determinate;

7.5. *controlul ierarhic permanent, răspunderea personală și profesionalismul* – deciziile nu sunt pur automatizate, orice concordanță biometrică este verificată manual de personal calificat, care poartă răspundere personală pentru validitatea datelor;

7.6. *transparența și respectarea secretului de stat și a altor informații cu accesibilitate limitată* - se asigură monitorizarea legalității prin jurnalizare (log-uri), protejând în același timp confidențialitatea investigațiilor și informațiile clasificate.

8. În exercitarea atribuțiilor specifice privind căutarea și schimbul de date, PUC aplică principii operaționale prevăzute la art. 4 din Lege.

Secțiunea a 2-a
Structura organizatorică a PUC

9. Funcțiile PUC sunt exercitate de către Direcția cooperare polițienească internațională a Inspectoratului General al Poliției (*în continuare – DCPI*), care reprezintă platforma unică responsabilă de coordonarea strategică și operațională la nivel național, monitorizarea fluxurilor de informații și asigurarea cooperării polițienești internaționale în regim de 24/7.

10. Structura internă a PUC include următoarele subdiviziuni specializate ale DCPI:

10.1. *Punctul Național de Contact Europol* – asigură la nivel național, schimbul de date și informații prin intermediul Router-ului și al sistemului EPRIS, în calitate de structură desemnată pentru coordonarea operațională, transmiterea și recepționarea solicitărilor, în condițiile competențelor prevăzute de cadrul normativ aplicabil;

10.2. *Biroul Național Central Interpol* – asigură interfața cu baza de date SLTD privind documente de călătorie, vizele, inclusiv a celor declarate false, furate sau pierdute, precum și a datelor privind permisele de conducere;

10.3. *Secția 24/7* – responsabilă de asigurarea fluxului informațional permanent și monitorizarea disponibilității sistemelor;

10.4. *Secția cooperare polițienească* – coordonează schimbul de date și informații în contextul evenimentelor majore cu dimensiune transfrontalieră;

10.5. *Biroul național SIRENE* – gestionează și coordonează alertele în cadrul Sistemului de Informații Schengen, asigurând schimbul de informații suplimentare legate de aceste alerte în conformitate cu procedurile prevăzute în Manualul SIRENE.

Secțiunea a 3-a
Atribuțiile și funcțiile PUC

11. PUC reprezintă platforma națională centralizată de coordonare operațională și administrativă a schimbului de informații, asigurând punctul unic de contact între autoritățile de aplicare a legii naționale și infrastructura centrală a Uniunii Europene, prin utilizarea infrastructurii de comunicații securizate și a celorlalte mecanisme de interoperabilitate tehnică, juridică și organizațională. În exercitarea acestei funcții, PUC acționează ca structură de gestionare a fluxurilor informaționale, fiind desemnată la nivel național pentru a asigura schimbul securizat de date cu statele membre ale Uniunii Europene, alte state și organizațiile internaționale profilate pe prevenirea și combaterea criminalității, având următoarele atribuții funcționale și operaționale principale:

11.1. asigurarea notificării oficiale către Comisia Europeană, Secretariatul General al Consiliului Uniunii Europene, Agenția eu-LISA și Europol, în termen de cel mult o lună de la data desemnării, cu privire la identitatea și datele de legătură ale PUC și a Punctelor Naționale de Contact (*în continuare – PNC*) pe domenii de competență, precum și cu privire la identitatea autorității de supraveghere a prelucrării datelor cu caracter personal ori a autorităților judiciare competente, a listei limbilor stabilite pentru schimbul de informații conform pct. 44, inclusiv a oricăror modificări ulterioare ale acestora, în vederea publicării în Jurnalul Oficial al Uniunii Europene sau pe platformele online dedicate ale Comisiei;

11.2. primirea, analizarea și soluționarea cererilor de informații transmise de autoritățile naționale și străine, inclusiv furnizarea informațiilor solicitate sau din proprie inițiativă ori de câte ori sunt relevante pentru prevenirea sau investigarea infracțiunilor;

11.3. direcționarea solicitărilor către autoritățile competente și coordonarea procesului de furnizare a datelor, asigurând sincronizarea fluxurilor de informații prin Biroul național Sirene, Punctul Național de Contact Europol și Biroul Național Central Interpol;

11.4. coordonarea schimbului de profiluri ADN, date dactiloscopice și imagini faciale prin intermediul Router-ului UE, facilitând interogarea bazelor de date biometrice naționale și internaționale;

11.5. realizarea schimbului de date și informații prin sistemul EPRIS, utilizând instrumentul de căutare pentru interogarea registrelor naționale de evidențe ale

poliției, inclusiv a datelor nominale privind persoanele urmărite, dispărute fără veste sau implicate în activități infracționale, pe baza indicilor de evidență polițienească;

11.6. realizarea schimbului de date dactiloscopice prin intermediul Router-ului, pe baza interogărilor automatizate ale bazelor de date naționale de dactiloscopie, în cooperare cu Punctul Național de Contact competent, cu respectarea condițiilor și procedurilor stabilite de legislația națională și de tratatele internaționale la care Republica Moldova este parte;

11.7. realizarea căutărilor automatizate și a schimbului de date prin sistemul EUCARIS, utilizând ca identificatori numărul de identificare a vehiculului (VIN), numărul de înmatriculare, numărul de motor sau numărul de serie al piesei componente, pentru accesarea datelor privind proprietarii sau utilizatorii vehiculelor și a informațiilor tehnice referitoare la starea juridică a mijloacelor de transport;

11.8. gestionarea operativă a alertelor în Sistemul de Informații Schengen referitoare la bunuri, mijloace de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale și documente de înmatriculare raportate ca fiind furate sau pierdute;

11.9. realizarea schimbului operativ de date și informații prin utilizarea canalelor de comunicare securizate ale Interpol, în vederea verificării în baza de date SLTD a documentelor de călătorie, vizelor, inclusiv a celor declarate false, furate sau pierdute, pe baza informațiilor puse la dispoziție de autoritățile competente;

11.10.gestionarea, la nivel de coordonare și schimb de informații, a procedurilor de dare în urmărire internațională, de localizare a persoanelor dispărute fără veste în contextul cauzelor penale sau din motive umanitare, de identificare a cadavrelor sau a părților acestora, precum și a procedurilor de predare/preluare a persoanelor urmărite sau căutate, desfășurate prin canalele de cooperare polițienească internațională, în condițiile competențelor prevăzute de cadrul normativ aplicabil;

11.11.asigurarea accesului efectiv al personalului desemnat din cadrul PNC sau al altor autorități de aplicare a legii, pentru cooperarea cu Europol la toate bazele de date stabilite expres prin lege sau prin acte normative aplicabile, în limitele competențelor, scopului determinat, necesității și proporționalității, în limitele competențelor legale, pentru a permite schimbul rapid de date și informații privind infracțiunile transfrontaliere, inclusiv traficul ilicit de vehicule și alte forme de criminalitate organizată relevante;

11.12.asigurarea suportului informațional și de coordonare pentru operațiuni comune, supravegheri și urmăriri transfrontaliere, desfășurate prin canalele de cooperare polițienească internațională, în colaborare cu autoritățile competente;

11.13.informarea, la cerere, a statului furnizor cu privire la prelucrarea datelor cu caracter personal transmise și la rezultatele operative obținute în urma utilizării acestora în cadrul investigațiilor naționale.

12. În vederea asigurării bunei funcționări a schimbului de date și informații conform standardelor Prüm II, PUC îndeplinește următoarele funcții de management operațional și monitorizare a utilizării:

12.1. monitorizarea operativă a disponibilității sistemelor și notificarea imediată a eu-LISA, Europol și a statelor membre în cazul unor defecțiuni tehnice

sau a indisponibilității infrastructurii naționale, pe baza informațiilor furnizate de PNC tehnice;

12.2. supravegherea utilizării standardului UMF pentru toate schimburile de date, în vederea garantării uniformității și interoperabilității fluxului informațional la nivel de utilizator;

12.3. efectuarea operativă a interogărilor simultane în CIR prin intermediul ESP în cazurile de terorism sau infracțiuni grave, utilizând interfețele tehnice puse la dispoziție de administratorii de sistem;

12.4. agregarea și transmiterea indicatorilor statistici către CRRS gestionat de eu-LISA și către instituțiile europene abilitate, pe baza datelor colectate și furnizate obligatoriu de către PNC.

13. În scopul consolidării cooperării polițienești internaționale, conducătorul PUC are următoarele responsabilități de coordonare internațională:

13.1. participă, cel puțin o dată pe an, la reuniunile organizate la nivelul Uniunii Europene cu șefii punctelor de contact unice din celelalte state membre ale Uniunii Europene;

13.2. evaluează, în cadrul acestor reuniuni, calitatea cooperării dintre serviciile naționale și cele străine;

13.3. analizează și propune măsurile tehnice sau organizatorice necesare în cazul apariției unor dificultăți în schimbul de informații;

13.4. contribuie la clarificarea și armonizarea procedurilor operaționale de schimb de date și informații în conformitate cu standardele europene;

13.5. facilitează schimbul de experiență, de cunoștințe de specialitate, precum și de informații generale și tehnice privind prevenirea și combaterea criminalității, asigurându-se că aceste schimburi se extind asupra metodelor și celor mai bune practici de prevenire și nu includ date cu caracter personal.

Secțiunea a 4-a
Modul de organizare și funcționare al PUC

14. PUC asigură adoptarea tuturor măsurilor tehnice și organizatorice pentru disponibilitatea permanentă a sistemelor informatice, funcționând în regim de 24 de ore pe zi, 7 zile pe săptămână. Astfel garantând capacitatea de a recepționa, evalua și furniza răspunsuri la cererile de informații în termenele de urgență stabilite.

15. PUC utilizează conectivitatea tehnică securizată necesară schimbului de date și informații cu infrastructurile externe, asigurată potrivit Hotărârii Guvernului nr. 65/2026 cu privire la conectarea Republicii Moldova la rețeaua TESTA și cadrului normativ aplicabil.

16. Pentru funcționarea adecvată, eficientă și rapidă a schimbului de informații, autoritatea în cadrul căreia este instituit PUC asigură acestuia:

16.1. personal calificat și instruit periodic în utilizarea SIENA și a sistemului de gestionare a cazurilor;

16.2. instrumente operaționale și resurse tehnice adecvate sarcinilor de serviciu;

16.3. resurse financiare și infrastructură necesare mentenanței sistemelor;

16.4. capacități de traducere necesare pentru a furniza răspunsuri în termenele imperative stabilite la pct. 28.

17. În scopul asigurării unui schimb de informații adecvat și rapid, PUC asigură personalului accesul la programe de formare periodică, ce includ în mod obligatoriu:

17.1. utilizarea instrumentelor tehnice (SIENA și sistemul de gestionare a cazurilor);

17.2. aplicarea legislației privind protecția datelor și a standardelor de confidențialitate;

17.3. utilizarea limbilor de lucru notificate Comisiei Europene, cu accent deosebit pe perfecționarea competențelor de comunicare în limba engleză, pentru a permite procesarea cererilor și furnizarea răspunsurilor în termenele de urgență stabilite.

18. Toate operațiunile de acces și schimb de date și informații sunt înregistrate în Sistemul electronic unic de gestionare a cazurilor, care este un sistem informațional de stat, deținut de Ministerul Afacerilor Interne și administrat de Inspectoratul General al Poliției. Sistemul servește drept instrument central de triaj, evidență și monitorizare, asigurând trasabilitatea acțiunilor și a termenelor de prelucrare a cererilor de informații și a răspunsurilor, precum și interoperabilitatea tehnică deplină cu aplicația securizată SIENA, garantând că orice comunicare primită prin SIENA este înregistrată direct în sistem, iar orice comunicare expediată prin SIENA este trimisă direct din sistem, permițând corelarea automată a numerelor de caz internaționale cu dosarele de investigație naționale.

19. Autoritatea care administrează Sistemul electronic unic de gestionare a cazurilor se asigură că toate riscurile de securitate cibernetică referitoare la acesta, în special în ceea ce privește arhitectura, guvernanța și controlul sistemului, sunt gestionate și abordate într-un mod prudent și eficient. În acest scop, administratorul de sistem implementează garanții adecvate împotriva accesului neautorizat și a abuzului, asigurând integritatea, disponibilitatea și confidențialitatea datelor prelucrate în conformitate cu standardele europene și legislația națională privind securitatea cibernetică.

Secțiunea a 5-a
Condiții pentru solicitarea și schimbul de informații

20. PUC asigură faptul că orice cerere de informații transmisă către alt stat membru al Uniunii Europene sau alte state, este necesară și proporțională cu scopul urmărit și că informațiile solicitate sunt disponibile în statul respectiv.

21. În conformitate cu cerințele de necesitate și proporționalitate, PUC se asigură că cererile de informații sunt transmise către statele membre ale Uniunii Europene sau alte state, numai în cazul în care:

21.1. există motive obiective care justifică că informațiile solicitate sunt necesare și proporționale pentru prevenirea, depistarea sau investigarea infracțiunilor;

21.2. există motive obiective care justifică că informațiile sunt disponibile în statul membru solicitat;

21.3. cererea indică și motivează caracterul urgent, în special dacă datele sunt esențiale pentru prevenirea unei amenințări directe și iminente la viața și sănătatea unei persoane sau există riscul pierderii relevanței acestora.

22. Cererile de informații transmise de PUC trebuie să conțină cel puțin următoarele elemente:

22.1. identificarea solicitantului: denumirea autorității solicitante, data și numărul de înregistrare al solicitării;

22.2. specificarea informațiilor solicitate: o descriere cât mai detaliată a datelor necesare în circumstanțele date;

22.3. scopul și justificarea: descrierea detaliată a scopului cererii, a faptelor investigate și a modului de operare, cu indicarea infracțiunii a cărei pregătire sau săvârșire face obiectul investigației;

22.4. legătura cu persoana vizată: precizarea detaliată a legăturii de cauzalitate dintre scopul solicitării și persoana fizică sau juridică ori entitate la care se referă informațiile, incluzând datele de identificare necesare (nume, prenume, data nașterii, cetățenie, serie/număr act);

22.5. motivele disponibilității: motivele obiective pentru care se consideră că statul solicitat deține informațiile respective;

22.6. regimul de urgență: precizarea caracterului de urgență (dacă este cazul) și motivarea obiectivă a acestuia, conform criteriilor de la pct. 26;

22.7. restricții de utilizare: precizarea oricăror restricții privind utilizarea informațiilor conținute în cerere în alte scopuri decât cele pentru care a fost transmisă cererea.

23. În cazul în care o autoritate de aplicare a legii desemnată transmite o cerere de informații sau furnizează informații în temeiul unei astfel de cereri direct unei autorități competente dintr-un alt stat membru al Uniunii Europene sau alt stat, potrivit procedurii prevăzute la art. 6 alin. (5) din Lege, aceasta are obligația de a transmite simultan, o copie a cererii sau a informațiilor respective către PUC, precum și către punctul de contact unic al celuilalt stat membru al Uniunii Europene sau alt stat.

24. Prin derogare de la pct. 23, autoritatea de aplicare a legii desemnată poate decide să nu transmită copia simultană către PUC exclusiv în situații excepționale și temeinic justificate, în cazul în care acest fapt ar periclita:

24.1. o investigație extrem de sensibilă în desfășurare, pentru care prelucrarea informațiilor necesită un nivel adecvat de confidențialitate;

24.2. un caz de terorism care nu implică situații de urgență sau de gestionare a crizelor;

24.3. siguranța unei persoane.

25. Autoritatea de aplicare a legii care a aplicat derogarea are obligația de a informa PUC și de a transmite copia solicitării imediat ce circumstanțele excepționale care au justificat măsura nu mai există.

26. PUC marchează cererea ca fiind urgentă în situația în care informațiile solicitate îndeplinesc una sau mai multe dintre următoarele condiții:

26.1. sunt esențiale pentru prevenirea unei amenințări imediate și grave la adresa siguranței statului/publice;

26.2. sunt necesare pentru prevenirea unei amenințări directe și iminente la adresa vieții sau integrității fizice a unei persoane;

26.3. sunt necesare pentru adoptarea unei decizii care poate implica menținerea unor măsuri restrictive care echivalează cu privarea de libertate;

26.4. există un risc iminent să își piardă relevanța, dacă nu sunt furnizate de urgență, și sunt considerate importante pentru prevenirea, depistarea sau investigarea infracțiunilor.

27. Datele privind vizele și titlurile de valoare, prevăzute la art. 6 alin. (2) lit. h) din Lege, au calitatea de informații indirect accesibile. Acestea sunt furnizate Punctului Unic de Contact de către autoritățile competente deținătoare, exclusiv în baza mecanismului solicitare-răspuns, prin utilizarea platformei de interoperabilitate MConnect sau a altor canale securizate.

Secțiunea a 6-a
Termene de furnizare a informațiilor și autorizarea judiciară

28. PUC furnizează informațiile solicitate în următoarele termene maxime:

28.1. ***8 ore*** pentru cereri urgente referitoare la informații direct accesibile;

28.2. ***3 zile calendaristice*** pentru cereri urgente referitoare la informații indirect accesibile;

28.3. ***7 zile calendaristice*** pentru toate celelalte cereri.

29. Derogarea de la termenele maxime stabilite la pct. 28 se permite exclusiv în situația în care respectarea acestora este imposibilă din cauza necesității obținerii unei autorizații judiciare sau din motive obiective de indisponibilitate a informațiilor solicitate. Se interzice prelungirea termenelor invocând volumul datelor sau complexitatea verificărilor, dacă acestea nu se încadrează în motivele obiective de imposibilitate de furnizare.

Durata maximă a prelungirii nu poate depăși durata termenului inițial prevăzut pentru categoria respectivă de cerere, cu excepția cazurilor în care este necesară obținerea unei autorizații judiciare, caz în care termenul se prelungește strict cu perioada necesară finalizării procedurii judiciare.

30. În situația în care termenele nu pot fi respectate în temeiul motivelor de derogare prevăzute la pct. 29, PUC aplică următoarele măsuri:

30.1. informează imediat autoritatea solicitantă despre întârziere, precizând motivele obiective (indisponibilitatea tehnică sau necesitatea autorizației judiciare) și furnizând o estimare a noului termen de răspuns;

30.2. furnizează informațiile parțial, pe măsură ce acestea devin disponibile, fără a aștepta soluționarea integrală a cauzei, dacă acest lucru este util investigației;

30.3. înregistrează justificarea prelungirii în Sistemul electronic unic de gestionare a cazurilor, indicând numărul autorizației judiciare sau natura impedimentului obiectiv, pentru audit și raportare statistică;

30.4. menține informată autoritatea solicitantă ori, după caz, punctul de contact unic din statul membru solicitant pe tot parcursul derulării procedurilor de obținere a autorizației judiciare și furnizează informațiile solicitate cât mai curând posibil după obținerea acesteia.

31. În cazul în care furnizarea informațiilor solicitate necesită, conform legislației naționale, obținerea unei autorizații judiciare, PUC și autoritățile de aplicare a legii aplică următoarele reguli de procedură:

31.1. nu se solicită autorizație judiciară pentru furnizarea de informații către un alt stat membru dacă legislația națională nu impune o astfel de procedură pentru

furnizarea de informații similare în context național, asigurându-se un tratament nediscriminatoriu al cererilor internaționale;

31.2. PUC sau autoritățile de aplicare a legii desemnate întreprind imediat toate măsurile necesare, pentru a obține autorizația judiciară în cel mai scurt timp posibil, în conformitate cu prevederile Codului de procedură penală;

31.3. obținerea autorizației judiciare se realizează prin următoarele mecanisme de competență și permanență:

31.3.1. autorizația judiciară este obligatorie pentru toate categoriile de informații care, conform Codului de procedură penală, necesită autorizarea judecătorului de instrucție;

31.3.2. cererea de autorizare se depune de către procuror la judecătorul de instrucție competent, conform normelor din legislația procesual-penală;

31.3.3. examinarea cererilor de autorizare judiciară se realizează prin mecanismele de permanență (24/7) instituite prin actele Consiliului Superior al Magistraturii, asigurându-se disponibilitatea imediată a autorităților judiciare la solicitarea PUC, astfel încât să fie garantată respectarea termenelor de urgență prevăzute de prezentul Regulament;

31.4. PUC informează imediat autoritatea solicitantă despre întârzierea preconizată cauzată de procedura judiciară, precizând motivele obiective și durata estimată a acesteia;

31.5. pe parcursul procedurii, PUC menține informată autoritatea solicitantă și furnizează informațiile imediat după obținerea autorizației judiciare, recurgând la furnizarea eșalonată a datelor dacă acestea devin disponibile parțial;

31.6. cererile de autorizare sunt evaluate și soluționate în conformitate cu legislația națională al statului solicitat/solicitant, după caz, asigurându-se că interesele esențiale ale securității naționale sau buna desfășurare a investigațiilor nu sunt periclitate;

31.7. autoritățile naționale au obligația de a asigura transmiterea informațiilor solicitate de către PUC după obținerea autorizației, pentru a permite încadrarea în limitele de timp impuse de standardele internaționale de cooperare;

31.8. în caz de urgență majoră, unde viața unei persoane este în pericol iminent, cererea de informații poate fi transmisă și verbal autorităților competente străine prin canalele PUC, urmând ca aceasta să fie confirmată în scris prin intermediul canalului SIENA sau al altor canale autorizate în termen de cel mult 24 de ore.

Secțiunea a 7-a
Refuzul cererilor și furnizarea din proprie inițiativă

32. PUC poate refuza furnizarea informațiilor dacă este aplicabil unul dintre următoarele motive:

32.1. informațiile nu sunt disponibile sau cererea nu îndeplinește cerințele de necesitate și proporționalitate, prevăzute la pct. 21;

32.2. autorizația judiciară necesară a fost refuzată;

32.3. furnizarea datelor ar periclita interesele securității naționale, buna desfășurare a unei investigații în desfășurare sau siguranța unei persoane sau ar prejudicia interesele legitime ale unei persoane juridice;

32.4. cererea vizează o infracțiune pentru care legea prevede o pedeapsă maximă de un an de închisoare conform legislației naționale sau o faptă care nu constituie infracțiune;

32.5. informațiile solicitate constituie date cu caracter personal care nu se încadrează în categoriile permise pentru schimbul internațional;

32.6. informațiile sunt inexacte, incomplete sau nu mai sunt actualizate;

32.7. informațiile provin de la un alt stat sau țară terță care nu și-a dat acordul pentru retransmiterea acestora;

32.8. există o încălcare vădită a drepturilor fundamentale ale omului.

33. Orice refuz de a da curs unei cereri de informații afectează numai partea din informațiile solicitate la care se referă motivele de refuz și nu aduce atingere obligației de a furniza celelalte părți ale informațiilor respective în conformitate cu prezentul Regulament.

34. În cazul în care informațiile solicitate nu pot fi obținute din motive legale (refuzul autorizației judiciare, restricții de securitate națională) sau tehnice (indisponibilitatea sistemelor, date necorespunzătoare calitativ), PUC aplică următoarele proceduri:

34.1. notificarea imediată: PUC informează autoritatea solicitantă în termenele prevăzute la pct. 28 despre imposibilitatea furnizării, precizând clar motivele refuzului sau natura defecțiunii tehnice;

34.2. indicarea duratei: în cazul problemelor tehnice, se comunică durata estimată pentru restabilirea sistemelor și, dacă este posibil, se propun modalități alternative de schimb (Interpol, bilateral);

34.3. înregistrarea refuzului: orice situație de imposibilitate a furnizării se înregistrează în Sistemul electronic unic de gestionare a cazurilor, cu menționarea motivului specific, în scopul raportării statistice către Comisia Europeană;

34.4. orice notificare de refuz sau comunicare aferentă se transmite în limba în care a fost primită cererea, conform regulilor de la pct. 44.

35. În cazul în care informațiile furnizate în cerere sunt insuficiente pentru a permite prelucrarea acesteia, PUC solicită imediat autorității solicitante clarificările sau precizările necesare, în absența cărora cererea se refuză.

36. Termenele de furnizare a informațiilor prevăzute la pct. 28 se suspendă din momentul în care autoritatea solicitantă primește cererea de clarificări, până în momentul în care clarificările solicitate sunt furnizate către PUC.

37. PUC furnizează din proprie inițiativă informațiile disponibile altor puncte de contact unice atunci când există motive obiective să considere că acestea sunt relevante pentru prevenirea, depistarea sau investigarea infracțiunilor grave.

38. Prevederile prezentului Regulament nu impun nicio obligație de a furniza informații în scopul utilizării acestora ca mijloace de probă în procedurile judiciare. Informațiile furnizate prin PUC nu pot fi utilizate ca mijloace de probă în procedurile judiciare fără acordul prealabil al statului care le-a furnizat, iar în cazul utilizării acestora în cadrul procesului penal, se aplică cu prioritate normele privind asistența juridică internațională în materie penală, conform principiului prevalenței asistenței juridice stabilit de lege.

Secțiunea a 8-a

Cerințe operaționale și managementul datelor

39. PUC își îndeplinește sarcinile în regim de 24/7. Accesul personalului PUC la informațiile disponibile este strict limitat la datele necesare pentru îndeplinirea atribuțiilor instituționale specifice, fiind exercitat în conformitate cu principiile necesității și proporționalității, cu respectarea Legii nr. 195/2024 privind protecția datelor cu caracter personal și a normelor speciale privind securitatea informațiilor cu accesibilitate limitată.

40. PUC, precum și toate PNC-urile care ar putea fi implicate în schimbul de informații, sunt conectate direct la aplicația securizată SIENA, inclusiv, după caz, prin dispozitive mobile securizate. Schimbul de informații și comunicarea operațională se realizează prin intermediul rețelei securizate TESTA, care asigură conectivitatea tehnică și transportul securizat al datelor. Accesul la aplicația SIENA, în special prin dispozitive mobile, este condiționat de aplicarea măsurilor stricte de securizare, autentificare multifactorială și monitorizare continuă a terminalelor, în conformitate cu cerințele tehnice europene.

41. PUC este autoritatea responsabilă de decizia privind canalul de cooperare utilizat pentru schimbul de informații, având competența de a selecta sau de a schimba canalul în scopul asigurării celei mai mari eficiențe, celerități și securități a schimbului. Decizia se bazează pe următoarele criterii și situații:

41.1. *prioritatea SIENA* – utilizarea implicită a aplicației securizate SIENA pentru schimburile cu statele membre și Europol;

41.2. *interoperabilitatea* – utilizarea altor canale securizate (Interpol, SELEC sau bilaterale) atunci când statul partener nu utilizează SIENA sau în cazul implicării unor țări terțe;

41.3. *urgența majoră* – utilizarea temporară a celui mai rapid canal disponibil pentru salvarea vieții sau integrității unei persoane;

41.4. *continuitatea* – utilizarea canalelor alternative în cazul unor incidente tehnice neașteptate care împiedică funcționarea SIENA.

42. Toate operațiunile de primire, prelucrare și furnizare a informațiilor efectuate de PUC sunt înregistrate într-un Sistem electronic unic de gestionare a cazurilor, ultimul asigurând:

42.1. *managementul centralizat* – înregistrarea tuturor cererilor, notificarea personalului, monitorizarea termenelor de 8h/3z/7z și corelarea cu numerele de caz internaționale din SIENA;

42.2. *funcția de triaj și prevenire* – verificarea automată a existenței unor solicitări anterioare pe același subiect în canalele SIRENE, Europol și Interpol pentru a preveni suprapunerea investigațiilor;

42.3. *trasabilitatea și auditul* – generarea înregistrărilor (log-urilor) care includ identificatorul utilizatorului, data/ora, bazele de date interogate și referința la dosarul penal, păstrate pentru o perioadă de 3 ani pentru controlul Centrul Național pentru Protecția Datelor cu Caracter Personal (*în continuare* – CNPDCP);

42.4. *protecția datelor* – asigurarea accesului prin autentificare multifactorială, ștergerea irevocabilă a datelor care nu mai sunt necesare și reexaminarea periodică a necesității păstrării acestora la cel mult 6 luni de la încheierea schimbului de informații.

43. Coordonarea fluxurilor informaționale se realizează prin procedura de triaj și înregistrare centralizată în Sistemul electronic unic de gestionare a cazurilor. PUC verifică în mod obligatoriu existența unor solicitări anterioare pe același subiect în canalele SIRENE, Europol și Interpol înainte de validarea unei noi cereri, asigurând astfel utilizarea celui mai eficient canal de cooperare și prevenirea suprapunerii activităților de investigare.

44. Schimbul de informații prin intermediul PUC se realizează în limba română în comunicarea cu autoritățile naționale și în limba engleză în relația cu partenerii internaționali și statele membre ale Uniunii Europene. În funcție de disponibilitate și de acordul prealabil al părților implicate în schimbul de date, pot fi utilizate și alte limbi de circulație internațională.

45. În cadrul schimburilor de informații reglementate de prezentul capitol, PUC asigură respectarea următoarelor standarde de calitate și protecție a datelor:

45.1. datele cu caracter personal furnizate sunt exacte, complete și actualizate;

45.2. categoriile de date furnizate sunt limitate la datele Europol relevante pentru executarea cererii și sunt transmise doar în măsura în care acestea sunt necesare și proporționale cu scopul urmărit;

45.3. odată cu furnizarea informațiilor, PUC transmite, în măsura posibilității, elementele necesare care să permită autorității solicitante să evalueze gradul de acuratețe, exhaustivitate și fiabilitate a datelor, precum și nivelul de actualizare a acestora.

46. Personalul PUC are obligația de a evalua, de la caz la caz, necesitatea transmiterii către Europol a unei copii a cererii de informații, a informațiilor furnizate în temeiul unei astfel de cereri sau a informațiilor furnizate din proprie inițiativă, în măsura în care informațiile respective vizează infracțiuni ce intră în sfera obiectivelor Europol.

47. În cazul în care, urmare a evaluării de la pct. 46, o copie este transmisă către Europol, PUC se asigură că scopurile prelucrării și orice restricții privind prelucrarea respectivă sunt comunicate în mod corespunzător agenției. Informațiile obținute inițial de la un alt stat sau de la o țară terță sunt transmise către Europol numai în cazul în care statul ori țara respectivă și-a dat acordul prealabil pentru această transmitere.

III. CADRUL OPERAȚIONAL PENTRU SCHIMBUL DE DATE

Secțiunea 1
Router-ul

48. În scopul facilitării stabilirii de conexiuni între Republica Moldova, statele membre ale Uniunii Europene și Europol, PUC utilizează serviciile Router-ului UE ca punct central de legătură pentru interogarea, extragerea și evaluarea automatizată a datelor biometrice, precum și pentru extragerea datelor alfanumerice.

49. Arhitectura tehnică utilizată de PUC prin intermediul Router-ului cuprinde următoarele componente naționale, administrate tehnic de către PNC-urile de domeniu responsabile de administrarea tehnică a segmentelor de date (Serviciul Tehnologii Informaționale, autoritate administrativă în subordinea MAI (*în continuare – STI*), Centrul tehnico-criminalistic și expertize judiciare (*în continuare – CTCEJ*)) și punctul de conectare la rețeaua TESTA (STISC)):

49.1. infrastructura centrală la nivel național, care include un instrument de căutare ce permite interogarea simultană a bazelor de date naționale și a datelor gestionate de Europol;

49.2. canalul securizat de comunicații între infrastructura centrală națională și autoritățile competente;

49.3. infrastructura de comunicații securizată (rețeaua TESTA) care asigură legătura cu ESP și serviciile Router-ului UE.

50. Competența PUC se limitează exclusiv la utilizarea operativă a Router-ului de către personalul autorizat pentru accesarea și schimbul de profiluri ADN, date dactiloscopice și imagini faciale. Configurarea, mentenanța și securitatea cibernetică a segmentelor tehnice naționale nu cad în sarcina PUC, fiind asigurate de PNC-urile de domeniu responsabile de administrarea tehnică a segmentelor de date (STI, CTCEJ) și punctul de conectare la rețeaua TESTA (STISC) conform atribuțiilor specifice detaliate în Anexa nr. 2.

Secțiunea a 2-a
Sistemul european de inventariere a evidențelor poliției (EPRIS)

51. Pentru căutarea de date în registrele naționale ale evidențelor poliției, PUC utilizează sistemul EPRIS ca infrastructură tehnică de interconectare descentralizată.

52. Sistemul EPRIS, pus la dispoziția PUC de către STI, autoritate administrativă în subordinea MAI, include următoarele componente obligatorii:

52.1. o infrastructură descentralizată instalată la nivel național, care asigură legătura tehnică cu sistemul central;

52.2. un instrument de căutare ce permite interogarea simultană a indexurilor registrelor naționale existente;

52.3. un canal de comunicații securizat între infrastructura națională și instrumentul de căutare.

53. Mecanismul de realizare a fluxului tehnic prin componentele prevăzute la pct. 52 se bazează pe următoarea arhitectură de interoperabilitate:

53.1. *segmentul național* – schimbul de date între nodul EPRIS și PUC se realizează prin intermediul platformei guvernamentale de interoperabilitate (MConnect), care servește drept strat de interconectare național ce alimentează interfața tehnică internațională;

53.2. *segmentul extern* – conectivitatea tehnică și transportul securizat al datelor către infrastructura centrală a Uniunii Europene sunt asigurate prin rețeaua securizată TESTA, administrată la nivel național de către STISC.

54. În cadrul sistemului EPRIS, PUC exercită funcții strict operative de lansare a interogărilor și monitorizare a rezultatelor. Administrarea tehnică a nodului EPRIS, funcționarea instrumentului de căutare și integritatea infrastructurii descentralizate sunt în responsabilitatea exclusivă a STI, în calitate de PNC de domeniu.

Secțiunea a 3-a
Formatul universal pentru mesaje (UMF)

55. În vederea asigurării unui schimb internațional de date și informații structurat și a interoperabilității tehnice, orice schimb de date și informații realizat de către PUC trebuie să utilizeze standardul privind UMF.

56. Rolul PUC în raport cu standardul UMF este de a garanta uniformitatea datelor transmise și recepționate la nivel operativ. Dezvoltarea, implementarea tehnică și actualizarea standardului UMF în cadrul bazelor de date și al infrastructurii naționale conectate revin PNC (STI, Agenția Servicii Publice, CTCEJ), în etapa de operare a sistemelor proprii.

57. Orice incident tehnic, defecțiune a infrastructurii hardware sau software ori eroare de conectivitate a Router-ului, EPRIS sau a canalelor TESTA va fi raportat imediat de către PUC către PNC-urile de domeniu sau, după caz, punctul de conectare TESTA responsabil, acesta din urmă având obligația restabilirii funcționării sistemelor.

IV. PROCEDURI OPERAȚIONALE ȘI INTEROPERABILITATE

Secțiunea 1

Proceduri de interogare și interoperabilitate cu sistemele Uniunii Europene

58. PUC este responsabil de efectuarea interogărilor în bazele de date ale statelor membre și în datele Europol, simultan cu interogările în CIR prin intermediul ESP, atunci când există motive rezonabile să se considere că datele privind un bănuit sau o victimă a unei infracțiuni cu caracter terorist ori a unei alte infracțiuni grave sunt stocate în respectivul registru.

59. Personalul autorizat al PUC solicită o interogare prin transmiterea de date biometrice către Router. Router-ul trimite solicitarea de interogare către bazele de date ale tuturor sau ale anumitor state membre și către datele Europol, în mod simultan cu datele transmise de utilizator, în conformitate cu drepturile sale de acces.

60. La primirea unei solicitări de interogare din partea Router-ului, PUC, în calitate de autoritate a statului solicitat, asigură efectuarea interogării în bazele de date naționale în mod automatizat și fără întârziere.

61. Orice rezultat al interogărilor efectuate în CIR, se transmite utilizatorului autorizat din cadrul PUC prin intermediul ESP, în conformitate cu specificațiile tehnice de interoperabilitate ale Uniunii Europene.

62. Toate concordanțele rezultate urmare a interogărilor automatizate în bazele de date naționale sunt transmise înapoi, în mod automatizat, către Router. PUC este informat în mod automat de către Router în cazul în care nu există nicio concordanță.

63. În cazul în care PUC, în calitate de autoritate a statului solicitant, solicită clasificarea rezultatelor și dacă arhitectura tehnică permite, Router-ul clasifică răspunsurile primite prin compararea datelor biometrice utilizate pentru interogare cu datele biometrice furnizate în răspunsurile de la statele membre solicitate sau de la Europol.

64. Router-ul returnează PUC, în calitate de utilizator al Router-ului, lista datelor biometrice între care s-a stabilit o concordanță și clasificarea acestora.

65. Procedura tehnică pentru interogarea prin intermediul Router-ului, formatul răspunsurilor, precum și normele tehnice pentru compararea și clasificarea

concordanțelor sunt stabilite în conformitate cu actele de punere în aplicare și specificațiile tehnice adoptate la nivelul Uniunii Europene.

66. Solicitările și răspunsurile referitoare la căutarea automatizată a imaginilor faciale prin intermediul Router-ului conțin numai datele strict necesare identificării solicitării, urmăririi fluxului de schimb și gestionării concordanței. Cerințele tehnice și procedurale aferente acestui schimb sunt conforme cu specificațiile tehnice de interoperabilitate stabilite la nivelul Uniunii Europene, asigurând minimizarea datelor prelucrate.

67. Pentru asigurarea conformității cu prevederile pct. 60 și 61, orice căutare și interogare automatizată realizată prin intermediul Router-ului, al ESP sau CIR, inclusiv cele care vizează date biometrice și imagini faciale, asigură jurnalizarea obligatorie a operațiunilor prin generarea unor înregistrări (log-uri) protejate împotriva modificării sau ștergerii neautorizate, păstrate pe o perioadă de minimum 5 ani. Pista de audit va stoca în mod automat: numărul cazului individual/dosarului penal, temeiul juridic al verificării, identificatorul de utilizator, data/ora exactă, tipul de date biometrice procesate și rezultatul concordanței transmise.

68. Statul solicitat verifică calitatea datelor transmise printr-o procedură automatizată și informează imediat PUC, prin intermediul Router-ului, atunci când datele sunt necorespunzătoare pentru o comparare automatizată.

69. Calitatea datelor transmise prin intermediul Router-ului este verificată printr-o procedură automatizată. În cazul în care datele sunt necorespunzătoare pentru efectuarea unei comparări automatizate, PUC, în calitate de autoritate a statului solicitat, informează fără întârziere statul membru solicitant prin intermediul Router-ului.

70. PUC are acces, prin intermediul Router-ului, la datele biometrice puse la dispoziția Europol de către țări terțe. În cazul în care o căutare conduce la o concordanță între datele transmise și cele furnizate de țări terțe și stocate de Europol, acțiunea ulterioară de schimb de date și informații se realizează prin intermediul canalelor de cooperare cu Europol, în condițiile stabilite de legislația națională în domeniul cooperării polițienești internaționale.

71. Căutările automatizate prevăzute în prezenta secțiune se efectuează exclusiv în cadrul unor cazuri individuale și în conformitate cu dreptul intern.

Secțiunea a 2-a
Proceduri specifice pentru Sistemul EPRIS

72. În scopul efectuării de căutări în registrele naționale ale evidențelor poliției prin intermediul EPRIS, în vederea identificării persoanelor reținute, bănuiților, învinuiților, condamnaților, în legătură cu infracțiuni pentru care legea statului solicitant prevede o pedeapsă cu închisoarea mai mare de un an, precum și a persoanelor dispărute fără veste, PUC utilizează cel puțin două dintre următoarele date:

72.1. prenumele;

72.2. numele;

72.3. data nașterii.

73. În cazul în care sunt disponibile, se pot utiliza suplimentar următoarele date:

73.1. pseudonimul (sau numele utilizat anterior);
73.2. cetățenia;
73.3. țara nașterii;
73.4. genul.

74. Datele nominative (nume, prenume, pseudonime) se transmit obligatoriu sub formă pseudonimizată, prin utilizarea unor serii alfanumerice care împiedică identificarea directă a persoanei la etapa de căutare.

75. La primirea unei solicitări de interogare din partea EPRIS, PUC, în calitate de autoritate a statului solicitat, asigură lansarea interogării în registrul național de evidențe ale poliției în mod automatizat și fără întârziere.

76. Atunci când personalul autorizat al PUC solicită o interogare prin sistemul EPRIS, acesta transmite datele biografice prevăzute la pct. 72. Sistemul EPRIS transmite cererea de interogare către registrele naționale ale evidențelor poliției din statele membre partenere și Europol, simultan cu datele transmise de PUC, în conformitate cu drepturile de acces stabilite.

77. Toate concordanțele rezultate urmare a interogărilor în registrul național de evidențe ale poliției sunt trimise înapoi, în mod automatizat, către EPRIS.

78. Lista concordanțelor, precizând calitatea acestora și statul deținător al datelor, este returnată către PUC de către sistemul EPRIS în mod automatizat.

79. La primirea listei de concordanțe, PUC decide cu privire la rezultatele pentru care este necesară o acțiune ulterioară și transmite statului solicitat, prin intermediul canalului SIENA, o solicitare motivată cuprinzând datele biografice necesare și informațiile suplimentare relevante.

80. În cazul în care este imposibil din punct de vedere tehnic să se utilizeze EPRIS din cauza unei defecțiuni a infrastructurii Europol, PUC recepționează notificarea automatizată și informează autoritățile naționale competente.

La recepționarea notificării, PUC informează imediat Punctele Naționale de Contact și autoritățile de aplicare a legii desemnate despre indisponibilitatea sistemului central, în vederea suspendării interogărilor automatizate și activării canalelor alternative de cooperare (SIENA) până la remedierea situației de către Europol.

81. În cazul unei defecțiuni a infrastructurii naționale care face imposibilă utilizarea EPRIS, PUC notifică automatizat statele membre, Comisia Europeană și Europol și întreprinde imediat măsuri pentru restabilirea sistemului.

Secțiunea a 3-a
Proceduri specifice pentru Sistemul EUCARIS

82. Căutările automatizate în datele privind mijloacele de transport prin intermediul sistemului EUCARIS pot fi efectuate exclusiv prin utilizarea unui număr complet de identificare a vehiculului (VIN), a unui număr complet de înmatriculare, a unui număr de motor sau a numărului de serie al piesei componente identificabile ale acestora. Aceste căutări se realizează în conformitate cu legislația națională a statului solicitant pentru prevenirea și cercetarea infracțiunilor, precum și în scopul prevenirii, depistării și investigării infracțiunilor.

În cadrul sistemului EPRIS și al schimburilor de evidențe ale poliției, interogările și răspunsurile utilizează exclusiv numere de referință naționale

anonimizate (identificatori unici de dosar/evidență), care nu permit identificarea directă a persoanei vizate în faza de căutare automatizată. Structura și atribuirea numerelor de referință se realizează în conformitate cu standardele tehnice europene UMF.

83. Schimbul automatizat de date prin interfața EUCARIS permite accesul autorităților competente la următoarele seturi de date de referință din registrele naționale:

83.1. date privind proprietarii sau, după caz, utilizatorii vehiculelor;

83.2. date tehnice privind vehiculele și starea juridică a acestora. Orice accesare a acestor date jurnalizată automat în înregistrări (log-uri) pentru monitorizarea legalității, conform prevederilor prezentului Regulament, asigurându-se că datele privind proprietarii sunt furnizate exclusiv în privința persoanelor care au calitatea de bănuit, învinuit, inculpat sau condamnat, conform art. 15 alin. (3) din Lege.

Secțiunea a 4-a
Confirmarea concordanțelor și schimbul setului de date de bază

84. În cazul în care o căutare automatizată indică o concordanță (hit), PUC recepționează notificarea automatizată conținând datele de referință corespunzătoare.

85. Orice concordanță identificată în cadrul interogărilor automatizate în cazul datelor biometrice, este supusă unei revizuiri manuale efectuate de către cel puțin un expert sau specialist în domeniu din cadrul CTCEJ, calificat potrivit legislației naționale și procedurilor interne aplicabile, în scopul confirmării validității acesteia pe baza datelor de referință primite.

86. Setul de date de bază se returnează prin intermediul Router-ului în termen de maximum 48 de ore de la îndeplinirea cumulativă a următoarelor condiții:

86.1. concordanța a fost confirmată manual conform pct. 85;

86.2. a fost transmisă o descriere a faptelor și a fost indicată infracțiunea de bază, utilizând tabelul comun al categoriilor de infracțiuni stabilit la nivelul Uniunii Europene, în vederea evaluării proporționalității cererii în conformitate cu legislația națională.

87. Prin derogare de la pct. 86, termenul poate fi prelungit strict cu o perioadă necesară pentru obținerea unei autorizații judiciare, în cazul în care legislația națională condiționează transmiterea datelor de o astfel de autorizație.

88. În cazul datelor identificate, datele de bază cuprind, în măsura disponibilității:

88.1. numele, prenumele;

88.2. data nașterii;

88.3. pseudonimele;

88.4. cetățenia;

88.5. locul și țara nașterii;

88.6. genul;

88.7. data și locul obținerii datelor biometrice;

88.8. infracțiunea aferentă;

88.9. numărul cauzei penale;

88.10.autoritatea responsabilă.

89. În cazul datelor neidentificate sau al urmelor, setul de date de bază se limitează la data/locul obținerii datelor, infracțiunea pentru care au fost obținute, numărul cauzei penale și autoritatea responsabilă.

90. Decizia de a returna datele de bază nu poate fi luată exclusiv prin mijloace automatizate și este supusă verificării și aprobării de către o persoană autorizată.

Secțiunea a 5-a
Proceduri privind căutarea persoanelor dispărute fără veste în contextul cauzelor penale sau din motive umanitare și identificarea cadavrelor

91. Căutarea persoanelor dispărute fără veste în contextul cauzelor penale sau din motive umanitare se realizează prin interogarea bazelor de date naționale și internaționale la solicitarea autorităților competente în contextul victimelor catastrofelor naturale, accidentelor aviatice, feroviare sau în alte situații de urgență unde viața ori sănătatea persoanei este în pericol.

92. În scopul salvării vieții, protejării sănătății persoanei sau identificării cadavrelor și a părților acestora, prin excepție de la regulile generale de acces, este permis accesul automatizat prin intermediul sistemelor Router și EPRIS inclusiv la datele privind victimele sau martorii.

93. Interogările utilizează datele nominale, biometrice și antropometrice disponibile, fiind limitate strict la datele necesare identificării persoanei sau a cadavrului în cadrul unui caz individual determinat.

Secțiunea a 6-a
Proceduri în caz de indisponibilitate tehnică

94. PUC informează fără întârziere statele membre partenere, Comisia Europeană, Agenția eu-LISA și Europol despre orice indisponibilitate a schimbului de date, pe baza notificărilor primite de la PNC sau de la autoritățile competente. În exercitarea mandatului său, PUC comunică extern exclusiv informațiile relevante pentru stadiul cooperării, fără a prelua sarcini de diagnosticare sau remediere tehnică. Notificarea va include natura defecțiunii tehnice și durata estimată pentru restabilirea funcționării.

95. PUC are rolul de a coordona aceste acțiuni la nivel operativ, stabilind, în colaborare cu autoritățile tehnice și în conformitate cu legislația Uniunii Europene, modalități alternative temporare pentru schimbul de informații, pentru a asigura continuitatea fluxurilor de date.

96. PNC sau autoritățile competente deținătoare ale infrastructurii afectate întreprind imediat toate măsurile tehnice și organizatorice necesare pentru restabilirea funcționării sistemelor informatice.

97. În cazul în care utilizarea Router-ului ori a sistemului EPRIS este imposibilă din cauza unei defecțiuni a infrastructurii centrale gestionate de eu-LISA sau, respectiv, de Europol, PUC recepționează notificarea automatizată transmisă de aceste agenții.

La recepționarea notificării, PUC informează imediat Punctele Naționale de Contact și autoritățile de aplicare a legii desemnate despre indisponibilitatea

sistemului central, în vederea suspendării interogărilor automatizate și utilizării canalelor alternative de cooperare până la remedierea situației.

V. MANAGEMENTUL DATELOR, SECURITATEA ȘI JURNALIZAREA

Secțiunea 1

Securitatea sistemelor și a prelucrării datelor

98. Autoritățile competente și PNC, conform domeniilor de competență, asigură securitatea prelucrării datelor cu caracter personal în cadrul segmentelor de infrastructură națională pe care le gestionează și care sunt conectate la Router-ul UE și sistemul EPRIS. PUC coordonează și monitorizează la nivel operațional integritatea acestui schimb, cooperând cu eu-LISA și Europol.

99. În cazul unui incident de securitate care afectează Router-ul, PUC și Punctele Naționale de Contact tehnice cooperează imediat cu agenția eu-LISA și cu statele membre afectate pentru a asigura un răspuns rapid, eficace și adecvat.

În calitatea sa de stat nemembru conectat la infrastructura centrală, Republica Moldova, prin intermediul PUC, respectă planul de gestionare a incidentelor furnizat de eu-LISA și implementează măsurile de remediere sau izolare a segmentului național, după caz, pentru a proteja integritatea întregului sistem.

100. În cazul unui incident de securitate care are sau poate avea un impact asupra funcționării EPRIS ori asupra disponibilității, integrității și confidențialității datelor transmise prin acesta, PUC cooperează imediat cu statele membre partenere și cu Europol pentru a asigura un răspuns rapid, eficace și adecvat.

Informațiile privind incidentul sunt furnizate de către PUC statelor membre și Europol fără întârziere și sunt raportate în conformitate cu planul de gestionare a incidentelor furnizat de Europol, în vederea izolării riscurilor și protejării indexurilor naționale de evidențe polițienești.

101. Fără a aduce atingere obligațiilor de raportare internațională, PUC și PNC au obligația de a notifica fără întârzieri nejustificate grupul interinstituțional de coordonare strategică și Centrul Național pentru Protecția Datelor cu Caracter Personal despre orice incident de securitate care afectează componentele naționale ale Router-ului ori ale sistemului EPRIS.

Notificarea trebuie să includă o descriere a naturii incidentului, categoriile de date afectate, măsurile de remediere întreprinse, pentru a permite grupului interinstituțional evaluarea impactului operațional și formularea propunerilor de politici necesare, conform atribuțiilor prevăzute la art. 7 alin. (3) din Lege, precum și pentru a permite exercitarea atribuțiilor de supraveghere și control de către autoritatea de protecție a datelor.

102. PUC comunică fără întârziere Comisiei Europene, agenției eu-LISA și Europol orice incident de securitate care are sau poate avea un impact asupra operării ori disponibilității componentelor naționale ale Router-ului sau ale sistemului EPRIS, ori care periclitează integritatea și confidențialitatea datelor prelucrate prin acestea.

103. Furnizarea informațiilor și raportarea incidentelor menționate la pct. 94 se realizează în conformitate cu planul de gestionare a incidentelor furnizat de eu-LISA (pentru Router) și, respectiv, de Europol (pentru EPRIS), asigurând informarea

statelor membre partenere pentru a minimiza impactul asupra continuității schimbului automatizat de date.

104. Prelucrarea datelor cu caracter personal se realizează în conformitate cu Legea nr. 195/2024 privind protecția datelor cu caracter personal și cu standardele Uniunii Europene aplicabile în domeniul cooperării polițienești.

105. În scopul protejării infrastructurii tehnice, autoritatea competentă sau PNC implementează următoarele măsuri de securitate în cadrul sistemelor proprii:

105.1.protecția fizică a echipamentelor și instalațiilor de prelucrare a datelor;

105.2.împiedicarea accesului neautorizat la suporturile de date și echipamentele de prelucrare;

105.3.utilizarea mecanismelor de autentificare securizată (nume de utilizator individuale și coduri de acces) pentru personalul autorizat;

105.4.aplicarea tehnicilor de criptare corespunzătoare pentru transportul datelor către infrastructurile centrale;

105.5.asigurarea planurilor de redresare în caz de dezastru pentru restabilirea funcționării sistemelor.

106. PUC monitorizează aplicarea acestor măsuri și este informat imediat de către PNC despre orice incident cu impact asupra securității, asigurând raportarea acestuia către CERT-UE și autoritățile internaționale competente în termen de maximum 24 de ore de la detectarea incidentului.

Secțiunea a 2-a
Jurnalizarea și păstrarea înregistrărilor (log-urilor)

107. PUC asigură păstrarea înregistrărilor (log-urilor) tuturor operațiunilor de acces și schimb de date și informații efectuate prin sistemele automatizate pentru o perioadă de 3 ani de la data creării acestora, cu excepția înregistrărilor prevăzute la alin. (5) art. 43 din Lege, care se păstrează pentru termenul special stabilit de acestea. La expirarea termenului de păstrare, datele înregistrate se șterg imediat.

108. Înregistrările operațiunilor trebuie să conțină cel puțin următoarele informații:

108.1.entitatea care a inițiat solicitarea (stat membru, Europol sau autoritate națională);

108.2.data și ora transmiterii solicitării și a primirii răspunsului;

108.3.sistemele de informații și bazele de date interogate;

108.4.identificatorul unic al persoanei autorizate care a efectuat sau a solicitat căutarea;

108.5.justificarea interogării, inclusiv numărul de referință al dosarului sau al cauzei penale;

108.6.statutul procesual persoanei vizate de interogare (bănuit, învinuit, condamnat, victimă, persoană dispărută fără veste, cadavru sau părțile acestuia), conform art. 42 alin. (2) din Lege.

109. Înregistrările (log-urile) sunt utilizate exclusiv pentru monitorizarea protecției datelor, verificarea legalității prelucrării, asigurarea securității sistemelor și elaborarea de statistici.

Secțiunea a 3-a

Exactitatea, relevanța și procedura de marcare a datelor

110. În cazul constatării furnizării unor date incorecte, neactuale sau care nu ar fi trebuit furnizate, PUC notifică imediat autoritatea destinatară, precum și toate autoritățile naționale beneficiare cărora le-au fost puse la dispoziție datele respective, asigurând corectarea sau ștergerea acestora fără întârzieri nejustificate, în vederea evaluării impactului asupra procedurilor penale sau administrative aflate în desfășurare.

111. În cazul în care o persoană vizată contestă exactitatea datelor, PNC-ul deținător al datelor de referință aplică imediat un indicator specific (marcaj). PUC are obligația de a transmite acest marcaj către partenerii internaționali ori de câte ori datele respective sunt obiectul unui schimb, până la clarificarea situației de către autoritatea competentă.

112. Marcajul indică faptul că datele se află sub rezerva unei contestații și limitează utilizarea acestora până la clarificarea situației, putând fi eliminat doar cu acordul persoanei vizate sau în baza unei decizii judiciare ori a autorității de supraveghere. În sensul prezentului Regulament, marcarea datelor contestate constituie o măsură de blocare a prelucrării acestora în scopul protejării drepturilor persoanei vizate.

113. În cadrul schimbului automatizat de date biometrice și alfanumerice, PUC asigură catalogarea datelor de referință prin aplicarea unor numere de referință care permit identificarea și corelarea rezultatelor pozitive (hit), fără a limita prelucrarea ulterioară a acestora în scopul investigării infracțiunilor.

114. PUC asigură ștergerea imediată din Sistemul electronic unic de gestionare a cazurilor și din canalele de comunicare a oricăror date cu caracter personal despre care se constată că au fost primite sau furnizate ilegal.

115. Prin derogare de la obligația de ștergere, în cazul în care există motive întemeiate să se considere că ștergerea datelor ar aduce atingere intereselor legitime ale persoanei vizate, PUC restricționează prelucrarea datelor în locul ștergerii acestora. Datele a căror prelucrare a fost restricționată pot fi prelucrate ulterior exclusiv în scopul care a împiedicat ștergerea lor.

116. Datele cu caracter personal primite sau furnizate legal de către PUC se șterg irevocabil din evidențele sale operative:

116.1. imediat ce se constată că nu mai sunt necesare pentru scopul pentru care au fost schimbate, dar nu mai târziu de 6 luni de la încheierea schimbului de informații;

116.2. la primirea unei notificări de la PNC privind expirarea termenului de păstrare în registrul sursă, conform legislației naționale;

116.3. după expirarea perioadei pentru care datele Europol pot fi prelucrate ori stocate în scopul pentru care au fost transmise;

116.4. imediat după afișare, în cazul rezultatelor interogărilor automatizate care nu au generat o concordanță (no-hit) sau a concordanțelor care nu au fost confirmate manual conform procedurilor de validare.

117. PUC reexaminează necesitatea și conformitatea păstrării datelor în termen de cel mult 6 luni de la încheierea fiecărui schimb de informații și, ulterior, în mod regulat, pentru a asigura respectarea principiilor necesității și proporționalității, ștergând irevocabil datele care nu mai sunt necesare.

Secțiunea a 4-a
Protecția persoanelor vizate, monitorizarea și răspunderea

118. PUC, în cooperare cu autoritățile competente care au dreptul de a utiliza mecanismele de căutare și schimb automatizat de date, implementează măsuri de automonitorizare pentru a verifica conformitatea tuturor activităților de prelucrare cu Legea nr. 195/2024 privind protecția datelor cu caracter personal. Aceste măsuri includ verificarea anuală a înregistrărilor (log-urilor) și a justificărilor legale introduse în Sistemul electronic unic de gestionare a cazurilor, în conformitate cu prevederile art. 48 alin. (2) din Lege, pentru a asigura trasabilitatea deplină a fiecărui schimb de date și informații.

119. CNPDCP exercită controlul asupra prelucrărilor efectuate de PUC și PNC, cooperând activ cu Autoritatea Europeană pentru Protecția Datelor în cadrul responsabilităților lor de supraveghere a Router-ului și a sistemului EPRIS.

120. În scopul asigurării unei supravegheri coordonate a aplicării prezentului Regulament și a protecției datelor biometrice transmise prin intermediul Router-ului și al sistemului EPRIS, Centrul Național pentru Protecția Datelor cu Caracter Personal participă la reuniuni de supraveghere coordonată cu autoritățile de supraveghere ale statelor membre și cu Autoritatea Europeană pentru Protecția Datelor, cel puțin o dată la doi ani. Participarea are ca scop armonizarea practicilor de control, evaluarea legalității transferurilor de date și elaborarea capitolelor naționale pentru rapoartele de activitate ale Comitetului European pentru Protecția Datelor.

121. La cererea unei persoane vizate, PUC, în strânsă colaborare cu autoritatea competentă deținătoare a datelor (PNC), furnizează informații privind categoriile de date prelucrate, originea acestora și temeiul legal al prelucrării. În cazul în care persoana contestă exactitatea datelor, PUC asigură aplicarea marcajului în fluxul internațional, conform deciziei PNC sau a CNPDCP.

122. În cazul în care persoana vizată contestă exactitatea datelor prelucrate prin PUC și aceasta nu poate fi stabilită imediat, datele respective sunt marcate cu un indicator specific până la clarificarea situației, marcaj care poate fi eliminat doar cu acordul persoanei sau în baza unei decizii a autorității competente.

123. Persoana vizată poate depune o cerere de rectificare sau ștergere a datelor direct la PNC deținător al datelor sau prin intermediul PUC. PNC are obligația de a examina cererea și de a informa persoana vizată despre decizia luată în termen de maximum 30 de zile calendaristice. Pe toată durata examinării, datele rămân marcate și cu utilizare restricționată. În cazul unui refuz, persoana vizată poate ataca decizia la autoritatea de supraveghere (CNPDCP) sau în instanța de contencios administrativ, conform legislației.

124. Încălcarea dispozițiilor prezentului Regulament atrage după sine răspunderea în condițiile legislației.

VI. RAPORTARE ȘI INDICATORI STATISTICI
Secțiunea 1
Colectarea și furnizarea datelor statistice

125. În scopul evaluării eficienței cooperării polițienești internaționale, monitorizării legale și auditului securității, autoritățile competente/PNC, conform domeniului de competență, colectează și furnizează indicatorii statistici rezultați din utilizarea Router-ului, sistemului EPRIS și EUCARIS, iar PUC asigură agregarea și transmiterea acestora către organismele europene.

126. Până la data de 1 martie a fiecărui an, PUC furnizează Comisiei Europene statisticile privind schimburile de informații cu alte state membre efectuate în anul calendaristic precedent, utilizând datele agregate din Sistemul electronic unic de gestionare a cazurilor, în format anonimizat.

127. Această raportare vizează exclusiv managementul informațiilor și cuprinde în mod obligatoriu, următoarele categorii:

127.1.numărul de cereri de informații transmise și primite de către PUC și de către autoritățile de aplicare a legii desemnate;

127.2.numărul de răspunsuri furnizate, defalcate în cereri urgente și neurgente și pe state membre solicitante;

127.3.numărul de cereri refuzate, defalcate pe state membre solicitante și pe motivele de refuz;

127.4.statisticile privind respectarea termenelor de 8 ore/3 zile/7 zile și impactul autorizațiilor judiciare asupra acestora, defalcate pe state membre solicitante.

128. Autoritățile competente desemnate în calitate de PNC au obligația de a colecta și de a furniza către PUC toate datele necesare pentru elaborarea rapoartelor statistice, conform domeniului lor de specialitate (biometrie, mijloace de transport, evidențe ale poliției), asigurându-se că informațiile transmise nu permit identificarea persoanelor vizate.

Secțiunea a 2-a
Indicatori statistici specifici sistemelor de schimb automatizat (Router, EPRIS și EUCARIS)

129. Pentru schimbul automatizat de date biometrice (profiluri ADN, date dactiloscopice și imagini faciale) prin intermediul Router-ului, PUC colectează următoarele date:

129.1. numărul de interogări efectuate de Republica Moldova și numărul de interogări primite de la fiecare stat membru și de la Europol, pe categorii de date;

129.2. numărul de interogări efectuate în fiecare dintre bazele de date conectate la Router;

129.3. numărul de concordanțe (hits) identificate în bazele de date naționale și în cele ale partenerilor;

129.4. numărul de concordanțe confirmate manual care au generat schimbul setului de date de bază;

129.5. numărul de concordanțe confirmate în cazul cărora nu a avut loc schimbul de date de bază;

129.6. numărul de interogări lansate simultan în CIR prin intermediul Router-ului;

129.7. tipul concordanțelor identificate, clasificate astfel:

129.7.1. date identificate (persoană) – date neidentificate (urme);

129.7.2. date neidentificate (urme) – date identificate (persoană);

129.7.3. date neidentificate (urme) – date neidentificate (urme);

129.7.4. date identificate (persoană) – date identificate (persoană).

130. Pentru schimbul de evidențe ale poliției prin sistemul EPRIS, indicatorii statistici includ:

130.1. numărul de interogări efectuate și primite de către autoritățile competente naționale;

130.2. numărul de interogări efectuate în fiecare dintre registrele de evidențe ale poliției conectate;

130.3. numărul de concordanțe pozitive identificate în registrele naționale și străine.

131. Pentru schimbul de date și informații privind mijloace de transport prin sistemul EUCARIS, indicatorii statistici includ:

131.1. numărul total de interogări lansate de PUC și primite de la statele membre ori Europol, defalcate pentru fiecare stat membru și pentru Europol;

131.2. numărul de interogări în fiecare dintre bazele de date conectate la sistemul EPRIS;

131.3. numărul de concordanțe obținute în raport cu baza de date a fiecărui stat membru în parte.

Secțiunea a 3-a
Utilizarea și protecția rapoartelor statistice

132. Accesul la datele statistice este rezervat exclusiv personalului autorizat din cadrul PUC, Comisiei Europene, eu-LISA și Europol, în scopul elaborării politicilor operaționale și de asigurare a calității datelor.

În scopul monitorizării și evaluării cadrului de cooperare, PUC furnizează Comisiei Europene, Agenției eu-LISA și Europol informațiile și datele statistice necesare pentru elaborarea rapoartelor anuale și periodice de evaluare globală și de funcționare tehnică a Router-ului, sistemului EPRIS și EUCARIS. Informațiile furnizate cuprind în mod obligatoriu numărul de concordanțe confirmate în bazele de date naționale pentru fiecare categorie și tip de date.

Furnizarea informațiilor menționate se efectuează cu respectarea cerințelor de confidențialitate și nu trebuie să pericliteze metodele de lucru operaționale, să dezvăluie sursele, membrii personalului sau investigațiile aflate în desfășurare ale autorităților competente.

133. Datele statistice colectate sunt stocate după cum urmează:

133.1. indicatorii referitori la Router sunt transmiși și stocați în CRRS gestionat de eu-LISA;

133.2. indicatorii referitori la EPRIS sunt stocați de către Europol și PUC.

134. Este strict interzisă utilizarea datelor statistice pentru orice formă de identificare a persoanelor fizice, acestea fiind protejate prin măsuri tehnice și organizatorice împotriva utilizării neautorizate.

Anexa nr. 2 la Hotărârea Guvernului
nr. _____ /2026

REGULAMENTUL
privind organizarea și funcționarea Punctelor Naționale de Contact în scopul schimbului de date și informații

I. DISPOZIȚII GENERALE

1. Regulamentul de organizare și funcționare a Punctelor Naționale de Contact în scopul schimbului de date și informații (*în continuare – Regulament*) stabilește cadrul normativ pentru organizarea, funcționarea și atribuțiile Punctelor Naționale de Contact (*în continuare – PNC*), precum și procedurile operaționale pentru schimbul de date biometrice (profiluri ADN, date dactiloscopice și imagini faciale); date referitoare la vehicule, inclusiv autovehiculele anunțate în căutare, precum și piesele componente ale acestora consemnate cu număr de identificare, urmărite internațional sau fiind obiecte ale faptelor ilegale; date privind documentele de călătorie, vizele, titlurile de valoare și permisele de conducere, inclusiv cele declarate false, furate sau pierdute; informații privind criminalitatea economică și financiară; evidențe ale poliției, inclusiv datele nominale privind persoanele urmărite, dispărute fără veste, aflate în vizorul autorităților de aplicare a legii sau implicate în activități infracționale; datele biometrice și antropometrice necesare identificării persoanelor dispărute fără veste, a cadavrelor și a părților de cadavru; date care nu privesc persoanele și informații operative; datele cu caracter personal prelucrate în contextul evenimentelor majore cu dimensiune transfrontalieră și al prevenirii și combaterii infracțiunilor cu caracter terorist, precum și alte date și informații prevăzute la art. 2 alin. (4) din Legea nr. 209/2026 privind cooperarea polițienească internațională (*în continuare – Lege*).

2. PNC sunt autoritățile/instituțiile publice competente responsabile de gestionarea tehnică și administrarea schimbului pentru o categorie specifică de date.

3. Noțiunile și termenii utilizați în prezentul Regulament, care nu sunt definiți în mod specific în cuprinsul acestuia, au semnificația stabilită la pct. 5 din Regulamentul de organizare și funcționare a Punctului Unic de Contact (*în continuare – PUC*) în scopul schimbului de date și informații, prevăzut în Anexa nr. 1.

4. În sensul prezentului Regulament, sunt PNC următoarele autorități/instituții publice competente, responsabile de gestionarea bazelor de date naționale și furnizarea informațiilor către PUC:

4.1. ***Centrul tehnico-criminalistic și expertize judiciare (în continuare – CTCEJ) al Inspectoratului General al Poliției*** — pentru domeniile de profiluri ADN, date dactiloscopice și imagini faciale, în partea ce ține de examinarea, verificarea și validarea de specialitate a concordanțelor;

4.2. ***Serviciul Tehnologii Informaționale, autoritate administrativă în subordinea MAI (în continuare – STI)*** — în calitate de deținător și administrator tehnic al resurselor informaționale specializate, responsabil de asigurarea interfețelor tehnice pentru schimbul de date pentru domeniul evidențelor cu caracter criminal, contravențional, datele nominale privind persoanele urmărite, dispărute

fără veste sau implicate în activități infracționale, în condițiile și limitele prevăzute la art. 20-22 din Lege, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, precum și pentru datele dactiloscopice (în partea asigurării funcționării Sistemului informațional automatizat „Registrul de stat dactiloscopic" și a comunicațiilor aferente schimbului de date dactiloscopice);

4.3. ***Inspectoratul General de Carabinieri, autoritate administrativă în subordinea MAI*** (***în continuare – IGC)*** – pentru domeniul evenimentelor majore cu dimensiune transfrontalieră;

4.4. ***Agenția Servicii Publice (în continuare – ASP)*** — pentru domeniul de date privind mijloacele de transport, date privind documentele de călătorie, inclusiv a celor declarate false, furate sau pierdute, precum și date privind permisele de conducere;

4.5. ***Serviciul de Informații și Securitate (în continuare – SIS)*** — pentru informațiile necesare prevenirii infracțiunilor cu caracter terorist, în regim de informații indirect accesibile, în condițiile, limitele și conform procedurilor prevăzute de legislația națională;

5. PNC au obligația de a asigura interoperabilitatea sistemelor proprii cu infrastructura națională prin utilizarea prioritară a platformei guvernamentale de interoperabilitate (MConnect) pentru schimbul de date pe segmentul național către Sistemul electronic unic de gestionare a cazurilor administrat de către PUC, asigurând respectarea principiului „Digital by Default".

Obligația dezvoltării și punerii la dispoziție a interfețelor de interoperabilitate (servicii web de consum) necesare recepționării, integrării și consumului de date în cadrul Sistemului electronic unic de gestionare a cazurilor revine PUC, în calitate de administrator al sistemului central, în colaborare cu Agenția de Guvernare Electronică.

Utilizarea MConnect se va face cu respectarea standardului UMF și a cerințelor de securitate stabilite de Agenția de Guvernare Electronică, fără a afecta conectivitatea tehnică securizată către rețeaua TESTA administrată de Serviciul Tehnologia Informației și Securitate Cibernetică (*în continuare – STISC*).

6. Fiecare autoritate desemnată în calitate de PNC, stabilește, prin act administrativ intern, subdiviziunea responsabilă de executarea nemijlocită a atribuțiilor și persoanele autorizate să efectueze verificările manuale.

II. PRINCIPIILE DE ACTIVITATE ALE PNC ȘI MANAGEMENTUL CALITĂȚII DATELOR

Secțiunea 1

Principii operaționale și de protecție a datelor

7. În exercitarea atribuțiilor specifice privind gestionarea tehnică și administrarea schimbului pentru o categorie specifică de date, PNC aplică principiile operaționale prevăzute la art. 4 din Lege precum și principiile de activitate stabilite în Secțiunea 1 a Anexei nr. 1, care se aplică în mod corespunzător.

8. PNC își desfășoară activitatea în baza următoarelor principii specifice prelucrării datelor biometrice și alfanumerice:

8.1. *principiul exactității și actualizării* — asigurarea caracterului veridic al datelor din registrele naționale și rectificarea sau ștergerea imediată a informațiilor incorecte;

8.2. *principiul calității datelor* — aplicarea procedurilor de verificare automatizată pentru a garanta că datele transmise permit compararea eficientă și reduc riscul concordanțelor false;

8.3. *principiul intervenției umane* — obligativitatea revizuirii manuale a oricărei concordanțe biometrice de către un membru calificat înainte de confirmarea hit-ului către PUC;

8.4. *principiul marcării datelor contestate* — aplicarea unui indicator special asupra datelor a căror exactitate este contestată de persoana vizată.

Secțiunea a 2-a
Calitatea datelor și standardele tehnice

9. PNC asigură că datele biometrice stocate (profiluri ADN, date dactiloscopice și imagini faciale) respectă standardele minime de calitate stabilite la nivelul Uniunii Europene pentru a permite compararea automatizată prin Router.

10. În cazul în care Router-ul notifică PUC că datele transmise de un PNC sunt necorespunzătoare pentru o comparare automatizată, PNC-ul vizat are obligația de a reexamina și de a corecta setul de date în cel mai scurt timp.

Secțiunea a 3-a
Interfețele tehnice pentru schimbul de date

11. Schimbul de date și informații între PNC și PUC, inclusiv în regim automatizat, se realizează prin intermediul platformei de interoperabilitate MConnect, care servește drept strat de interoperabilitate național ce alimentează interfețele tehnice internaționale, asigurând tranzitul securizat al datelor din registrele de stat către:

11.1. *Router-ul UE* – utilizat exclusiv pentru interogarea, extragerea și evaluarea automatizată a datelor biometrice (profiluri ADN, date dactiloscopice și imagini faciale);

11.2. *sistemul EPRIS* – utilizat ca infrastructură tehnică descentralizată pentru interconectarea și căutarea automatizată în registrele naționale de evidențe ale poliției;

11.3. *sistemul EUCARIS* – interfața specifică utilizată pentru schimbul automatizat al datelor privind mijloacele de transport;

11.4. *rețeaua securizată de comunicații TESTA* – infrastructură securizată de comunicații utilizată pentru asigurarea conectivității Republicii Moldova la canalele de schimb de date și informații ale Uniunii Europene și ale statelor participante, în scopul realizării schimbului automatizat de date și al cooperării polițienești internaționale, administrată la nivel național de autoritatea desemnată potrivit cadrului normativ;

12. În vederea asigurării unui schimb internațional de date și informații structurat și a interoperabilității tehnice, PNC-urile au următoarele obligații privind standardizarea:

12.1. la dezvoltarea și operarea infrastructurii naționale conectate la Router și EPRIS, PNC-urile utilizează obligatoriu standardul privind UMF;

12.2. orice schimb de date și informații trebuie să respecte specificațiile UMF pentru a garanta uniformitatea, structura și calitatea datelor transmise și recepționate la nivel național și european.

III. ADMINISTRAREA TEHNICĂ A INFRASTRUCTURII PENTRU SCHIMBUL DE DATE ȘI INFORMAȚII

Secțiunea 1
Administrarea tehnică a Router-ului și a bazelor de date biometrice

13. PNC conform domeniilor de competență, sunt responsabile de administrarea tehnică, mentenanța și securitatea nodului național conectat la Router-ul Uniunii Europene.

14. În raport cu infrastructura Router-ului, PNC-urile au următoarele obligații tehnice:

14.1. asigurarea interfeței tehnice a sistemelor proprii care conțin profiluri ADN, date dactiloscopice și imagini faciale cu Router-ul UE, facilitând interogarea automatizată;

14.2. implementarea și menținerea standardelor de calitate pentru datele biometrice stocate, asigurând proceduri de verificare automatizată a calității datelor transmise pentru a preveni erorile de comparare;

14.3. asigurarea conectivității tehnice securizate prin rețeaua TESTA, garantând disponibilitatea și securitatea canalului național de comunicații.

15. În timp ce PUC deține competența de utilizare operativă a rezultatelor, PNC-urile dețin competența tehnică exclusivă asupra infrastructurii hardware și software. PUC nu are atribuții în gestionarea bazelor de date biometrice, PNC-urile fiind singurele autorități responsabile de remedierea defecțiunilor care împiedică accesul Router-ului la datele de referință naționale.

Secțiunea a 2-a
Administrarea tehnică a Sistemului EPRIS

16. STI în calitate de PNC pentru domeniul evidențelor poliției, este responsabil de operarea tehnică a infrastructurii descentralizate a sistemului EPRIS la nivel național.

17. În exercitarea atribuțiilor prevăzute la pct. 16, STI asigură:

17.1. funcționarea și disponibilitatea infrastructurii tehnice naționale conectate la EPRIS;

17.2. interconectarea tehnică a indexurilor evidențelor poliției cu instrumentul de căutare EPRIS;

17.3. implementarea măsurilor tehnice de pseudonimizare, autentificare, control al accesului și securitate a comunicațiilor;

17.4. implementarea tehnică a drepturilor de acces aprobate de autoritățile competente;

17.5. jurnalizarea operațiunilor de acces, interogare și transmitere a rezultatelor, în condițiile cadrului normativ aplicabil;

17.6. notificarea PUC cu privire la incidentele tehnice și întreprinderea măsurilor necesare pentru restabilirea funcționării infrastructurii.

Secțiunea a 3-a
Implementarea tehnică a Standardului UMF

18. Toate PNC au obligația de a implementa și actualiza standardul privind UMF la nivelul bazelor de date sectoriale pe care le gestionează.

19. Implementarea tehnică a UMF la nivel de PNC presupune:

19.1. corelarea și organizarea structurată a informațiilor din registrele naționale conform specificațiilor tehnice europene, pentru a permite transportul acestora prin Router și EPRIS;

19.2. asigurarea interoperabilității automate, astfel încât mesajele generate de bazele de date naționale să poată fi procesate fără erori de sistemele internaționale;

19.3. actualizarea periodică a formatului UMF în conformitate cu specificațiile tehnice adoptate la nivelul Uniunii Europene, fără a depinde de intervenția operativă a PUC.

Secțiunea a 4-a
Mentenanța și garanția disponibilității

20. PNC-urile tehnice sunt responsabile de implementarea măsurilor de securitate fizică și logică (criptare, autentificare securizată) pentru protejarea integrității datelor în timpul procesului de transmitere către PUC.

21. PUC nu deține competențe sau resurse tehnice pentru intervenții asupra serverelor, bazelor de date sau rețelelor de comunicații. În cazul unui incident tehnic care afectează Router-ul, EPRIS sau utilizarea standardului UMF, PNC-ul responsabil are obligația de a interveni imediat pentru restabilirea funcționării și de a furniza detalii tehnice PUC pentru notificarea oficială a partenerilor internaționali și a CERT-UE.

IV. MANAGEMENTUL, RECTIFICAREA ȘI PROTECȚIA DATELOR

Secțiunea 1
Rectificarea și ștergerea datelor

22. În cazul în care un PNC constată că au fost furnizate către PUC date incorecte, neactuale sau care nu ar fi trebuit furnizate, acesta notifică imediat PUC pentru a asigura informarea partenerilor internaționali și rectificarea/ștergerea datelor în toate sistemele vizate.

23. Datele transmise legal se șterg în momentul în care nu mai sunt necesare pentru scopul transmiterii sau la expirarea termenului maxim de păstrare prevăzut de legislația națională.

24. PNC în calitate de operatori ai sistemelor informaționale și bazelor de date sectoriale, sunt exclusiv responsabile de monitorizarea legalității și a termenelor de păstrare a datelor de referință furnizate către PUC.

25. În cazul în care un PNC constată că datele furnizate anterior către PUC au fost transmise ilegal, sunt inexacte sau au fost șterse din registrele naționale ca urmare a expirării termenelor legale de păstrare, acesta notifică imediat PUC în

vederea ștergerii sau rectificării corespunzătoare a acestora în fluxurile internaționale.

26. Prin derogare de la obligația de ștergere prevăzută la pct. 22, în cazul în care există motive întemeiate să se considere că ștergerea datelor ar aduce atingere intereselor legitime ale persoanei vizate, PNC restricționează prelucrarea datelor în locul ștergerii acestora. Datele a căror prelucrare a fost restricționată pot fi prelucrate ulterior exclusiv în scopul care a împiedicat ștergerea lor.

27. PNC se asigură că orice set de date de bază furnizat către PUC în urma unei concordanțe (hit) respectă termenele maxime de păstrare prevăzute de legislația națională a Republicii Moldova, informând PUC cu privire la aceste termene la momentul furnizării.

Secțiunea a 2-a
Procedura de marcare a datelor (catalogare și blocare)

28. PNC asigură exactitatea și relevanța datelor cu caracter personal prelucrate prin aplicarea procedurilor de marcare corespunzătoare. În cadrul schimbului automatizat, PNC aplică procedura de catalogare pentru datele de referință, în scopul permiterii identificării și corelării acestora, fără a limita prelucrarea lor ulterioară.

29. Procedura de catalogare se realizează prin atribuirea unui număr de referință profilurilor ADN, datelor dactiloscopice și imaginilor faciale, în conformitate cu specificațiile tehnice prevăzute la art. 17 din Lege, permițând identificarea și corelarea rezultatelor pozitive (hit) fără a restricționa accesul sau prelucrarea datelor.

30. Dacă o persoană vizată contestă exactitatea datelor deținute de un PNC, iar aceasta nu poate fi stabilită imediat, PNC-ul aplică marcajul de blocare asupra datelor respective.

31. Marcajul de blocare limitează utilizarea datelor până la clarificarea situației și poate fi eliminat doar:

31.1. cu acordul expres al persoanei vizate;

31.2. în baza unei decizii definitive a instanței de judecată;

31.3. în baza unei decizii a Centrului Național pentru Protecția Datelor cu Caracter Personal (*în continuare – CNPDCP*).

Secțiunea a 3-a
Automonitorizarea și protecția persoanelor vizate

32. În calitate de operatori de date, PNC implementează proceduri interne de automonitorizare pentru a verifica dacă accesul PUC la datele de referință se realizează exclusiv în scopurile și condițiile prevăzute de lege.

33. PNC-urile au obligația de a pune la dispoziția CNPDCP toate înregistrările (log-urilor) păstrate pentru o perioadă de 3 ani, facilitând auditurile periodice privind legalitatea interogărilor automate primite prin intermediul Router-ului și EPRIS.

34. Atunci când PUC solicită informații în urma unei cereri a persoanei vizate, PNC-ul responsabil furnizează fără întârziere detaliile necesare pentru a demonstra exactitatea și relevanța datelor furnizate, sau procedează la rectificarea acestora dacă se constată erori.

V. JURNALIZAREA OPERAȚIUNILOR ȘI RAPORTAREA STATISTICĂ

Secțiunea 1
Păstrarea înregistrărilor (log-urilor)

35. Jurnalizarea operațiunilor de acces și schimb de date efectuate pe segmentul național între PNC și PUC este asigurată în mod automatizat prin intermediul platformei de interoperabilitate MConnect. Înregistrările (log-urile) sunt păstrate de către Agenția de Guvernare Electronică, în calitate de posesor al platformei, pentru o perioadă de 3 ani de la data creării acestora, asigurând PUC și CNPDCP accesul necesar pentru monitorizarea legalității prelucrării și auditul securității.

36. Înregistrările generate prin MConnect trebuie să asigure trasabilitatea conform standardelor prevăzute la pct. 105 din Anexa nr. 1, cuprinzând: entitatea solicitantă, data și ora exactă, bazele de date interogate, identificatorul persoanei autorizate și justificarea interogării. PNC-urile sunt exonerate de obligația instituirii unor sisteme de jurnalizare paralele pentru datele tranzitate prin MConnect, fiind responsabile doar de jurnalizarea acțiunilor de administrare locală a bazelor de date proprii.

Secțiunea a 2-a
Furnizarea indicatorilor statistici

37. Colectarea indicatorilor statistici privind numărul de interogări (lansate și primite) și timpul de răspuns pe segmentul național se realizează prin funcționalitățile integrate de raportare ale platformei MConnect. PUC are acces direct la aceste date agregate pentru elaborarea rapoartelor anuale destinate Comisiei Europene și eu-LISA, eliminând necesitatea furnizării manuale a acestor indicatori de către PNC-uri.

38. Indicatorii furnizați includ numărul de interogări primite/lansate pe categorii de date, numărul de concordanțe (hits) identificate și tipul acestora (persoană-persoană, persoană-urmă, etc.).

VI. SECURITATEA ȘI MANAGEMENTUL INCIDENTELOR

39. PNC-urile sunt responsabile de implementarea măsurilor de securitate pentru protejarea integrității și confidențialității datelor în timpul procesului de transmitere către PUC, prin:

39.1. *criptarea datelor* – PNC-urile utilizează tehnici de criptare corespunzătoare pentru transportul tuturor datelor către Router, EPRIS sau EUCARIS;

39.2. *autentificarea securizată* – accesul personalului autorizat din cadrul PNC-urilor la echipamentele de prelucrare se face exclusiv prin utilizarea numelor de utilizator individuale și a codurilor de acces confidențiale;

39.3. *protecția fizică și logică* – PNC-urile implementează măsuri care să împiedice citirea, copierea, modificarea sau ștergerea neautorizată a suporturilor de date în timpul transportului și prelucrării acestora.

40. În cazul unui incident semnificativ de securitate (impact asupra integrității sau confidențialității datelor), PNC notifică PUC imediat, pentru a permite raportarea către CERT-UE în termen de maximum 24 de ore.

41. Încălcarea dispozițiilor prezentului Regulament atrage după sine răspunderea în condițiile legislației.

VII. Centrul tehnico-criminalistic și expertize judiciare al Inspectoratului General al Poliției și Serviciul Tehnologii Informaționale al MAI

Secțiunea 1
Atribuțiile specifice în domeniul datelor biometrice

42. CTCEJ este autoritatea responsabilă de gestionarea și administrarea bazelor de date naționale privind profilurile ADN, datele dactiloscopice și imaginile faciale, având competența exclusivă de a genera și furniza datele de referință și seturile de date de bază necesare schimbului automatizat, inclusiv în scopul identificării persoanelor dispărute fără veste și a cadavrelor neidentificate în contextul cazurilor umanitare și situațiilor de urgență. În acest scop, CTCEJ asigură funcționarea și securitatea interfeței tehnice a sistemelor proprii cu Router-ul UE, facilitând accesul automatizat al partenerilor internaționali, prin intermediul infrastructurii gestionate de PUC.

43. STI are obligația de a implementa și menține standardele minime de calitate pentru datele biometrice stocate, asigurând o procedură de verificare automatizată pentru a garanta că datele transmise permit o comparare eficientă și reduc riscul concordanțelor false. În cazul în care Router-ul notifică faptul că datele transmise sunt necorespunzătoare pentru o comparare automatizată, CTCEJ are responsabilitatea de a reevalua și corecta setul de date în cel mai scurt timp posibil.

44. Punerea în aplicare a obligațiilor STI privind administrarea tehnică a nodului național conectat la Router-ul UE și asigurarea interfeței automate cu infrastructura centrală a Uniunii Europene pentru profilurile ADN, datele dactiloscopice și imaginile faciale este condiționată de data la care Republica Moldova va obține accesul juridic și tehnic la aceste mecanisme, în temeiul tratatelor internaționale încheiate sau de la data aderării la Uniunea Europeană.

Secțiunea a 2-a
Validarea rezultatelor și proceduri de schimb de date și informații

45. Conform principiului intervenției umane, CTCEJ are responsabilitatea exclusivă de a valida orice concordanță (hit) identificată automatizat, prin revizuire manuală efectuată de un membru calificat. Decizia de a permite transmiterea setului de date de bază aparține PNC (CTCEJ), care facilitează schimbul prin interfața PUC în termen de maximum 48 de ore, asigurând structurarea informațiilor conform standardului UMF.

46. După confirmarea manuală a concordanței, CTCEJ facilitează prin intermediul PUC schimbul setului de date de bază în termen de maximum 48 de ore, utilizând obligatoriu standardul UMF pentru structurarea informațiilor. Comunicarea solicitărilor motivate de informații suplimentare și a detaliilor aferente dosarelor penale se realizează prin canalul securizat SIENA.

Secțiunea a 3-a
Organizarea administrativă și raportarea statistică

47. STI stabilește, prin act administrativ, subdiviziunea internă responsabilă de gestionarea conexiunii la Router-ul UE și desemnează nominal persoanele autorizate să efectueze interogările și verificările manuale ale rezultatelor. Personalul autorizat va utiliza exclusiv mecanisme de autentificare securizată (nume de utilizator individuale și coduri de acces confidențiale) pentru accesul la date.

48. În scopul evaluării eficienței cooperării, CTCEJ colectează și furnizează periodic către PUC indicatorii statistici specifici, care includ: numărul de interogări (lansate și primite), numărul de concordanțe (hits) identificate în bazele de date de profil și tipul acestora (persoană-persoană sau persoană-urmă), asigurându-se că informațiile transmise nu permit identificarea directă a persoanelor vizate. Toate aceste operațiuni de acces sunt jurnalizate și păstrate în înregistrări (log-uri) pentru o perioadă de 3 ani.

VIII. Serviciul Tehnologii Informaționale, autoritate administrativă în subordinea Ministerului Afacerilor Interne

Secțiunea 1
Atribuțiile specifice în domeniul evidențelor poliției cu caracter criminal, contravențional și dactiloscopic

49. STI este desemnat în calitate de PNC responsabil pentru administrarea tehnică a sistemelor informaționale de stat din domeniul afacerilor interne ce conțin evidențe cu caracter criminal, contravențional și dactiloscopic, precum și pentru datele referitoare la autovehiculele anunțate în căutare și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale. În exercitarea acestor atribuții, STI are rolul de deținător și administrator tehnic al resurselor informatice specializate, inclusiv al Sistemului Informațional Automatizat „Registrul Informației Criminalistice și Criminologice” și al Registrului de stat dactiloscopic, asigurând disponibilitatea tehnică a acestora și interconectarea nodului național EPRIS cu bazele de date naționale menționate, în vederea furnizării către PUC a datelor de referință necesare schimbului internațional.

50. La primirea unei solicitări de interogare prin intermediul sistemului EPRIS, STI asigură, prin mecanisme automatizate și fără întârziere, inițierea căutării în registrele naționale de evidență utilizând seturile de date obligatorii (nume, prenume și data nașterii) și, după caz, datele suplimentare disponibile. Toate concordanțele rezultate sunt transmise automatizat către EPRIS pentru a fi puse la dispoziția statului solicitant.

51. Exercitarea atribuțiilor de operare tehnică a infrastructurii descentralizate a sistemului EPRIS și asigurarea interconectării registrelor naționale de evidență cu sistemele informatice ale statelor membre ale Uniunii Europene și Europol se vor realiza progresiv, pe măsura asigurării condițiilor juridice și tehnice necesare pentru conectarea la infrastructura centrală a Uniunii Europene.

Secțiunea a 2-a
Standarde tehnice și protecția datelor în sistemul EPRIS

52. În scopul protejării identității persoanelor vizate în etapa de căutare, STI are obligația de a asigura exclusiv procesul tehnic de pseudonimizare a datelor nominative (nume, prenume, pseudonime), utilizând serii alfanumerice care să împiedice identificarea directă până la momentul confirmării unei concordanțe. STI se asigură că orice schimb de date și informații respectă standardul UMF, garantând astfel interoperabilitatea tehnică și uniformitatea informațiilor transmise.

53. În cazul în care o interogare indică o concordanță, STI facilitează furnizarea setului de date suplimentare în urma unei solicitări motivate transmise prin intermediul canalului SIENA. STI are responsabilitatea exclusivă de a monitoriza permanent disponibilitatea infrastructurii naționale EPRIS și de a întreprinde imediat toate măsurile tehnice necesare pentru restabilirea funcționării în cazul unor defecțiuni. PUC va fi notificat imediat de către STI despre natura incidentului tehnic, exclusiv în scopul informării partenerilor internaționali, fără a prelua sarcini de diagnosticare sau intervenție tehnică.

54. În cazul unui incident semnificativ la nivelul nodului național EPRIS, STI are obligația de a implementa fără întârziere măsurile tehnice de remediere și de a acorda asistență prioritară experților Europol pentru diagnosticare. STI furnizează PUC toate detaliile tehnice necesare pentru ca acesta să poată informa Comisia Europeană și partenerii internaționali în termenul de maximum 24 de ore de la detectare.

Secțiunea a 3-a
Organizarea internă, jurnalizarea și raportarea

55. STI stabilește, prin act administrativ, subdiviziunea responsabilă de administrarea tehnică a nodului EPRIS și desemnează nominal persoanele autorizate să gestioneze accesul la registrele de evidență. Personalul autorizat utilizează exclusiv mecanisme de autentificare securizată, bazate pe nume de utilizator individuale și coduri de acces confidențiale, pentru a preveni prelucrarea neautorizată a datelor.

56. Trasabilitatea operațiunilor de acces la registrele gestionate de STI în scopul schimbului de date cu PUC este garantată prin jurnalizarea integrată în platforma MConnect. STI asigură corelarea identificatorilor de utilizator cu sistemele proprii de autentificare pentru a permite identificarea precisă a persoanei autorizate în log-urile centralizate.

IX. Inspectoratul General de Carabinieri, autoritate administrativă în subordinea Ministerului Afacerilor Interne

Secțiunea 1
Atribuțiile specifice, canale de comunicare și interoperabilitate tehnică

57. IGC este desemnat în calitate de PNC responsabil pentru domeniul evenimentelor majore cu dimensiune transfrontalieră, având rolul de a furniza și de a schimba informații, la solicitare sau din proprie inițiativă, cu PUC și entitățile similare din statele membre în scopul prevenirii infracțiunilor, menținerii ordinii și siguranței publice în contextul evenimentelor majore cu dimensiune transfrontalieră, precum și pentru gestionarea riscurilor asociate acestora.

58. Schimbul de informații (furnizare/solicitare) în cazul evenimentelor majore cu dimensiune transfrontalieră gestionate de IGC, se va efectua prin intermediul PUC și PNC privind competițiile sportive gestionate de IGC, care operează prin intermediul canalelor Europol și al mecanismelor europene de cooperare polițienească.

59. În exercitarea atribuțiilor sale, IGC furnizează informații referitoare la grupuri de persoane care prezintă o amenințare la adresa ordinii și securității publice, precum și date care nu privesc persoanele (informații generale și tehnice), ori date operative relevante pentru asigurarea securității în cadrul evenimentelor publice. Schimbul de date și informații se realizează cu respectarea principiilor necesității și proporționalității, asigurând un echilibru între cerințele de securitate și protecția drepturilor fundamentale.

60. Punerea în aplicare a obligațiilor IGC privind schimbul de informații în cazul evenimentelor majore cu dimensiune transfrontalieră prin intermediul mecanismelor europene de cooperare polițienească și utilizarea canalului SIENA pentru aceste fluxuri este condiționată de data la care Republica Moldova va obține accesul juridic și tehnic la aceste instrumente, în temeiul tratatelor internaționale încheiate sau de la data aderării la Uniunea Europeană.

61. Pentru schimbul de informații aferente interogărilor sau solicitărilor primite, IGC utilizează ca interfață principală de comunicare aplicația SIENA, sub coordonarea operativă a PUC, având obligația de a asigura interoperabilitatea sistemelor proprii de evidență cu infrastructura gestionată de PUC prin utilizarea standardului UMF pentru toate mesajele structurate transmise. Orice soluție tehnică implementată la nivelul IGC trebuie să permită transportul datelor prin canale criptate, asigurând integritatea informațiilor pe tot parcursul fluxului comunicațional.

Secțiunea a 2-a
Organizarea administrativă, jurnalizarea și statistica

62. IGC stabilește, prin act administrativ, subdiviziunea responsabilă de cooperarea internațională și desemnează nominal personalul autorizat să gestioneze solicitările de date. Accesul acestora la sistemele informaționale se realizează exclusiv prin mecanisme de autentificare securizată, fiind strict interzisă utilizarea conturilor generice.

63. Trasabilitatea operațiunilor de acces la registrele gestionate de IGC în scopul schimbului de date cu PUC este garantată prin jurnalizarea integrată în platforma MConnect. IGC asigură corelarea identificatorilor de utilizator cu sistemele proprii de autentificare pentru a permite identificarea precisă a persoanei autorizate în log-urile centralizate.

X. Agenția Servicii Publice
Secțiunea 1
Atribuțiile specifice în domeniul datelor privind mijloacele de transport, documentele de călătorie și al permiselor de conducere

64. ASP este desemnată în calitate de PNC responsabil de gestionarea bazelor de date naționale privind mijloacele de transport, a datelor referitoare la documentele

de călătorie, inclusiv a celor declarate false, furate sau pierdute, precum și a datelor privind permisele de conducere, în scopul furnizării informațiilor necesare PUC pentru schimbul internațional de date și informații. În exercitarea acestor atribuții, ASP asigură conexiunea tehnică a registrelor proprii cu sistemul EUCARIS pentru datele despre mijloacele de transport și facilitează interfața cu baza de date SLTD a Interpol pentru verificarea documentelor de călătorie.

65. ASP, în calitate de PNC, asigură transmiterea imediată a informațiilor necesare către Biroul național SIRENE, în vederea introducerii unei alerte în Sistemul de Informații Schengen în toate cazurile de raportare a furtului certificatelor de înmatriculare a vehiculelor.

66. ASP asigură lansarea și primirea interogărilor automatizate fără întârziere, garantând accesul autorităților competente la datele privind proprietarii de vehicule și statutul documentelor de călătorie. Căutările în bazele de date privind proprietarii sau deținătorii vehiculelor sunt permise exclusiv în privința persoanelor care au calitatea de bănuit, învinuit, inculpat sau condamnat, în conformitate cu prevederile art. 15 alin. (3) din Lege. Toate schimburile de date și informații realizate prin aceste interfețe tehnice trebuie să utilizeze standardul UMF pentru a asigura uniformitatea și interoperabilitatea informațiilor transmise către partenerii internaționali.

67. ASP asigură interfața tehnică și fluxul de date necesar pentru introducerea și gestionarea în Sistemul de Informații Schengen a alertelor referitoare la mijloacele de transport și documente (documente de călătorie, certificate de înmatriculare și permise de conducere) raportate ca fiind furate, pierdute, sustrase sau anulate.

Interfața tehnică gestionată de ASP pentru verificarea documentelor de călătorie vizează exclusiv statutul juridic al documentului (validitate, furt, pierdere) și nu permite accesul la datele biometrice stocate pe mediul electronic al documentului.

68. ASP asigură accesul PUC la datele din Registrul de stat al vehiculelor și Registrul de stat al conducătorilor de vehicule în scopul îndeplinirii sarcinilor specifice de combatere a criminalității legate de vehicule, conform cerințelor de cooperare prin canalul Europol.

69. Prevederile referitoare la schimbul automatizat de date prin interfața EUCARIS și gestionarea alertelor în Sistemul de Informații Schengen vor produce efecte juridice și tehnice depline de la data acordării accesului oficial al Republicii Moldova la aceste infrastructuri europene, până la acea dată ASP asigurând schimbul de date prin canalele de cooperare internațională disponibile.

Secțiunea a 2-a
Managementul calității datelor și securitatea prelucrării

70. ASP are obligația de a asigura exactitatea și actualizarea permanentă a datelor din registrele de stat aflate în posesie, procedând la rectificarea sau ștergerea imediată a informațiilor incorecte ori neactuale identificate în cursul schimbului de date. În cazul în care o persoană vizată contestă exactitatea datelor deținute de ASP, instituția aplică un marcaj corespunzător care limitează utilizarea acestora până la clarificarea situației conform procedurilor legale.

71. În conformitate cu legislația națională, ASP retrage alerta din registrul de căutare de îndată ce motivul de introducere a alertei asupra vehiculului sau a

documentului aferent încetează să mai existe, asigurând informarea imediată a PUC, sau după caz Biroului național SIRENE pentru actualizarea corespunzătoare în Sistemul de Informații Schengen.

72. Pentru protejarea confidențialității, accesul personalului ASP la sistemele de schimb de date și informații se realizează exclusiv prin mecanisme de autentificare securizată (nume de utilizator individuale și coduri de acces), fiind implementate măsuri de securitate fizică și logică pentru a preveni accesul neautorizat. În cazul detectării unui incident de securitate semnificativ, ASP notifică imediat PUC pentru a permite raportarea incidentului către CERT-UE în termen de maximum 24 de ore.

Secțiunea a 3-a
Organizarea internă, jurnalizarea și raportarea statistică

73. ASP stabilește, prin act administrativ, subdiviziunea internă responsabilă de executarea atribuțiilor de PNC și desemnează nominal persoanele autorizate să efectueze interogările și să gestioneze fluxul de date.

74. Trasabilitatea operațiunilor de acces la registrele gestionate de ASP în scopul schimbului de date cu PUC este garantată prin jurnalizarea integrată în platforma MConnect. ASP asigură corelarea identificatorilor de utilizator cu sistemele proprii de autentificare pentru a permite identificarea precisă a persoanei autorizate în log-urile centralizate.

75. ASP colectează și furnizează periodic către PUC indicatorii statistici necesari, care includ numărul total de interogări (lansate și primite) prin sistemul EUCARIS și baza de date SLTD, precum și numărul de concordanțe obținute. Raportarea statistică se realizează astfel încât să nu permită identificarea directă a persoanelor vizate, servind exclusiv evaluării eficienței cooperării polițienești internaționale.

XI. Serviciul de Informații și Securitate al Republicii Moldova
Secțiunea 1
Atribuțiile specifice în domeniul prevenirii infracțiunilor cu caracter terorist

76. SIS este desemnat în calitate de PNC responsabil pentru domeniul furnizării informațiilor necesare prevenirii infracțiunilor cu caracter terorist, exclusiv în cadrul mecanismului de schimb de date și informații aferente acestui domeniu. În exercitarea acestor atribuții, SIS are rolul de a furniza PUC datele de referință și seturile de date de bază necesare schimbului internațional de date și informații în contextul combaterii terorismului, exclusiv în baza mecanismului solicitare-răspuns, sau din proprie inițiativă, atunci când circumstanțele justifică în mod rezonabil concluzia că persoanele vizate pot săvârși infracțiuni cu caracter terorist. În ambele situații, furnizarea datelor se realizează exclusiv în regim de informații indirect accesibile, fără acordarea unui acces tehnic direct sau permanent la sistemele informaționale proprii și după evaluarea prealabilă de către Serviciu a legalității și oportunității divulgării acestora.

77. SIS asigură că furnizarea informațiilor se realizează cu respectarea strictă a principiilor necesității și proporționalității, vizând exclusiv prevenirea infracțiunilor cu caracter terorist. Activitatea PNC din cadrul SIS se desfășoară fără a aduce

atingere suveranității, securității sau ordinii publice a Republicii Moldova, respectând principiul protejării intereselor naționale.

Secțiunea a 2-a
Standarde tehnice și canale de comunicare

78. SIS asigură interoperabilitatea sistemelor proprii cu infrastructura tehnică gestionată de PUC, utilizând standardul UMF și SIENA pentru schimbul de informații suplimentare. Rolul PUC în acest proces este strict limitat la asigurarea interfeței tehnice și operative de comunicație, fără a deține competențe de coordonare, analiză sau intervenție în domeniul combaterii terorismului, care rămân în responsabilitatea exclusivă a SIS conform legislației speciale.

79. Pentru acțiunile ulterioare confirmării unei concordanțe (hit) sau pentru transmiterea solicitărilor motivate de informații suplimentare, SIS utilizează ca interfață principală de comunicare canalul SIENA. În situații de urgență majoră, unde datele sunt esențiale pentru prevenirea unei amenințări iminente la viața unei persoane, SIS colaborează cu PUC pentru urgentarea procedurilor de schimb de date și informații.

Secțiunea a 3-a
Securitatea, jurnalizarea și raportarea statistică

80. SIS este responsabil de securitatea fizică și informațională a bazelor de date sectoriale conectate la infrastructura de schimb, implementând mecanisme de autentificare securizată prin nume de utilizator individuale și coduri de acces confidențiale. În cazul detectării unui incident de securitate care afectează integritatea sau confidențialitatea datelor, SIS notifică imediat PUC pentru a permite raportarea către CERT-UE în termen de maximum 24 de ore.

81. Datele și informațiile relevante obținute anterior pornirii urmăririi penale sau în cadrul activităților de identificare, documentare și investigare a faptelor susceptibile de a constitui infracțiuni cu caracter terorist sunt furnizate de către Serviciul de Informații și Securitate exclusiv în regim de informații indirect accesibile, cu respectarea regimului juridic aplicabil informațiilor operative, informațiilor atribuite la secret de stat și/sau surselor specifice de informații, conform legislației naționale.

XII. Serviciul Tehnologia Informației și Securitate Cibernetică

Secțiunea 1
Atribuțiile specifice în calitate de punct de conectare la domeniul local la rețeaua TESTA

82. STISC exercită potrivit Hotărârii Guvernului nr. 65/2026 cu privire la conectarea Republicii Moldova la rețeaua TESTA rolul de punct de conectare la domeniul local la rețeaua de comunicații securizată a Uniunii Europene TESTA.

83. Platforma MConnect constituie canalul principal pentru furnizarea informațiilor direct accesibile către PUC, eliminând necesitatea unor conexiuni punct-la-punct între PUC și sistemele informatice deținute de PNC (ASP, STI, CTCEJ). În timp ce Agenția de Guvernare Electronică asigură cadrul tehnic de interoperabilitate și securitatea datelor în tranzit pe segmentul național, STISC

rămâne responsabil exclusiv de administrarea tehnică a rețelei securizate TESTA, asigurând legătura dintre nodul central național (alimentat prin MConnect) și infrastructura Uniunii Europene.

84. Funcțiile de administrare a infrastructurii securizate de comunicații S-TESTA pe segmentul de legătură cu infrastructura centrală a Uniunii Europene, precum și asigurarea suportului tehnic pentru funcționarea Router-ului UE, a sistemului EPRIS și a sistemului EUCARIS, se vor pune în aplicare de la data obținerii accesului tehnic și juridic al Republicii Moldova la resursele menționate.

Secțiunea a 2-a
Securitatea și managementul incidentelor de securitate

85. STISC asigură monitorizarea continuă a canalului național de comunicații pentru detectarea oricăror anomalii sau amenințări la adresa securității schimbului internațional de date și informații.

86. În cazul detectării unui incident semnificativ de securitate cibernetică care afectează disponibilitatea sau integritatea rețelei TESTA, STISC are următoarele obligații:

86.1. notifică imediat PUC despre natura și impactul incidentului, furnizând detaliile tehnice necesare pentru a permite raportarea către CERT-UE în termen de maximum 24 de ore;

86.2. întreprinde măsuri imediate de izolare a incidentului și de restabilire a funcționării canalelor de comunicații afectate;

86.3. colaborează cu eu-LISA și Europol, prin intermediul PUC, pentru implementarea planurilor de gestionare a incidentelor la nivel de rețea.

87. În cazul unui incident la nivelul Router-ului, STISC și PNC-urile de domeniu (STI, CTCEJ) au obligația de a acorda asistență tehnică prioritară experților eu-LISA, furnizând toate informațiile necesare pentru diagnosticare și aplicând fără întârziere corecțiile de securitate sau modificările de configurație solicitate prin planul de răspuns coordonat de agenție.

88. Trasabilitatea operațiunilor de acces la registrele gestionate de STISC în scopul schimbului de date cu PUC este garantată prin jurnalizarea integrată în platforma MConnect. STISC asigură corelarea identificatorilor de utilizator cu sistemele proprii de autentificare pentru a permite identificarea precisă a persoanei autorizate în log-urile centralizate.

NOTA DE FUNDAMENTARE

la proiectul de hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații

1. Denumirea autorului și, după caz, a participanților la elaborarea proiectului

Proiectul hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații.

2. Condițiile ce au impus elaborarea proiectului de act normativ

2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ

În temeiul art. 6 alin. (2), (6) și (7), art. 19 alin. (8), art. 22 alin. (2), art. 42 alin. (4) și art. 56 alin. (2) din Legea nr. 209/2026 privind cooperarea polițienească internațională .

Proiectul de hotărârii de Guvern este elaborat în scopul executării punctelor 53, 58 și 66 din capitolul 24 - „Justiție, Libertate și Securitate", Cluster 1. „Valori Fundamentale" din Programul național de aderare a Republicii Moldova la Uniunea Europeană (în continuare – UE) pentru anii 2025-2029, aprobat prin Hotărârea Guvernului nr. 306/2025.

Elaborarea proiectului de hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații este justificată de necesitatea asigurării transpunerii parțiale a:

1. Regulamentului (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024 privind căutarea și schimbul automatizat de date în scopul cooperării polițienești, și de modificare a Deciziilor 2008/615/JAI și 2008/616/JAI ale Consiliului și a Regulamentelor (UE) 2018/1726, (UE) 2019/817 și (UE) 2019/818 ale Parlamentului European și ale Consiliului (Regulamentul Prüm II);
2. Deciziei 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere;
3. Deciziei 2008/616/JAI a Consiliului din 23 iunie 2008 privind punerea în aplicare a Deciziei 2008/615/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere;
4. Directivei (UE) 2023/977 a Parlamentului European și a Consiliului din 10 mai 2023 privind schimbul de informații dintre autoritățile de aplicare a legii ale statelor membre și de abrogare a Deciziei-cadru 2006/960/JAI a Consiliului;
5. Deciziei 2004/919/CE a Consiliului din 22 decembrie 2004 privind combaterea criminalității referitoare la vehicule și având implicații transfrontaliere.

2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative

În contextul obținerii statutului de țară candidată pentru aderarea la UE la 23 iunie 2022, Republica Moldova este responsabilă de adaptarea infrastructurilor administrative și instituționale, precum și de armonizarea legislației naționale cu legislația UE în domeniile relevante.

Situația actuală evidențiază faptul că mecanismele naționale de schimb de date utilizate în cooperarea polițienească transfrontalieră – inclusiv datele ADN, datele dactiloscopice, datele privind înmatricularea vehiculelor, imaginile faciale și evidențele polițienești – nu sunt reglementate într-un mod unitar la nivelul unei legi speciale. În prezent, aceste mecanisme nu sunt structurate în logica „căutării automatizate" și a schimbului standardizat de informații, astfel cum este prevăzut de Regulamentul (UE) 2024/982 (Prüm II). În acest context, se conturează necesitatea stabilirii unor condiții și proceduri clare pentru realizarea căutărilor automatizate asupra acestor categorii de date, ca element esențial al alinierii la standardele europene în domeniul cooperării polițienești.

Proiectul de hotărârii de Guvern este elaborat în legătură cu necesitatea îndeplinirii măsurilor prioritare pentru consolidarea nivelului de pregătire a Republicii Moldova în procesul de aderare la UE și alinierea legislației naționale la acquis-ul UE, asigurării implementării integrale, calitative și în termen a recomandărilor formulate de Comisia Europeană, pentru îndeplinirea angajamentelor asumate în baza Acordului de Asociere între UE.

Activitățile infracționale transnaționale și terorismul necesită un răspuns coordonat și un schimb de date eficient și rapid.

În prezent, cadrul legal național care reglementează cooperarea polițienească internațională se bazează pe instrumente juridice care, deși funcționale, nu mai corespund dinamicii actuale a criminalității transfrontaliere și progresului tehnologic.

Evoluția amenințărilor transfrontaliere necesită instrumente care să permită identificarea rapidă a suspecților prin căutări automatizate în bazele de date ale altor state membre.

Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024 privind căutarea și schimbul automatizat de date în scopul cooperării polițienești, cunoscut și sub denumirea de Regulamentul Prüm II, este un act legislativ european major menit să consolideze securitatea internă în UE. Acest regulament face parte din pachetul UE privind codul de cooperare polițienească, propus de Comisia Europeană pentru a eficientiza lupta împotriva criminalității transfrontaliere.

Directiva (UE) 2023/977 a Parlamentului European și a Consiliului din 10 mai 2023, stabilește normele organizatorice și procedurale ale Uniunii Europene pentru a asigura un schimb de informații adecvat și eficient între autoritățile de aplicare a legii din statele membre ale UE în vederea prevenirii, depistării și investigării infracțiunilor.

Transpunerea acestor acte europene este imperativă pentru asigurarea continuității cooperării cu agențiile UE (precum Europol) și pentru menținerea statutului de partener de încredere în domeniul ordinii și securității publice.

În prezent, schimbul de informații între autoritățile de aplicare a legii din Republica Moldova și partenerii externi (în special UE) se realizează prin canale multiple, însă fragmentate. Principalul punct de contact este Direcția Cooperare Polițienească Internațională (DCPI) al Inspectoratului General al Poliției, care gestionează fluxurile prin INTERPOL, Europol (aplicația SIENA) și ofițerii de legătură.

Deși există o colaborare activă, procedurile sunt adesea manuale și nu sunt pe deplin integrate într-un flux de lucru automatizat care să respecte standardele stricte de timp impuse de noul acquis european.

3. Obiectivele urmărite și soluțiile propuse

3.1 Principalele prevederi ale proiectului și evidențierea elementelor noi

Obiectivul principal al proiectului de hotărârii de Guvern este să modernizeze schimbul de informații între autoritățile competente din statele membre, îmbunătățind mecanismele stabilite anterior.

La fel, stabilește condiții și proceduri pentru căutarea și schimbul automatizat de profile ADN, date dactiloscopice (amprente), datele de înmatriculare a vehiculelor, imagini faciale (o noutate importantă), înregistrări polițienești (prin intermediul unui nou sistem numit EPRIS).

Proiectul instituie Punctul Unic de Contact (PUC) în cadrul Inspectoratului General al Poliției, care va servi drept interfață centralizată între sistemele naționale și infrastructura Uniunii Europene.

Se desemnează Punctele Naționale de Contact (PNC) pe domenii de competență (ADN, dactiloscopie, imagini faciale, vehicule, evidențe polițienești).

Soluția tehnică include utilizarea Router-ului UE, a sistemului EPRIS și a rețelei EUCARIS**.**

Proiectul extinde arhitectura de interoperabilitate prin reglementarea utilizării componentelor tehnice centrale ale Uniunii Europene: Portalul European de Căutare (ESP), care permite interogarea simultană și rapidă a sistemelor informatice; Depozitul Comun de Date de Identitate (CIR), destinat identificării persoanelor și prevenirii utilizării identităților multiple; și Depozitul Comun de Raportare și Statistici (CRRS), necesar pentru monitorizarea performanței serviciilor și generarea rapoartelor agregate.

Un element pilon al proiectului este instituirea Sistemului electronic unic de gestionare a cazurilor, care servește drept instrument central de triaj, evidență și monitorizare a schimbului de informații. Acest sistem asigură interoperabilitatea tehnică deplină cu aplicația securizată SIENA, garantând trasabilitatea acțiunilor și corelarea automată a numerelor de caz internaționale cu dosarele de investigație naționale.

Schimbul de date pe segmentul național între Punctele Naționale de Contact (PNC) și Punctul Unic de Contact (PUC) este guvernat de principiul „Digital by Default”, fiind realizat prin intermediul platformei guvernamentale de interoperabilitate MConnect. Aceasta constituie stratul de interconectare național care alimentează automatizat interfețele tehnice internaționale.

Prezentul proiect de act normativ stabilește cadrul juridic și instituțional necesar pentru implementarea mecanismelor de schimb automatizat de date între Republica Moldova și statele membre ale Uniunii Europene, prin transpunerea parțială a Regulamentului (UE) 2024/982 (Prüm II) și a Directivei (UE) 2023/977.

Se reglementează rolul Biroului Național SIRENE în gestionarea alertelor din cadrul Sistemului de Informații Schengen (SIS), inclusiv obligația Agenției Servicii Publice de a furniza date imediate pentru introducerea alertelor privind documentele de înmatriculare, pașapoartele sau permisele de conducere raportate ca fiind furate, pierdute sau anulate.

În conformitate cu standardele europene de securitate, proiectul introduce obligația păstrării înregistrărilor (log-urilor) pentru operațiunile de căutare realizate prin intermediul Router-ului, ESP sau CIR pentru o perioadă de minimum 5 ani, asigurând o pistă de audit nealterabilă pentru monitorizarea legalității prelucrării.

Se instituie Punctele Naționale de Contact (PNC) pe domenii de competență, responsabile de furnizarea datelor din bazele de date sectoriale către PUC:

- ***Centrul Tehnico-Criminalistic și Expertize Judiciare al IGP*** - pentru domeniile de profiluri ADN, date dactiloscopice și imagini faciale, în partea ce ține de examinarea, verificarea și validarea de specialitate a concordanțelor;
- ***Serviciul Tehnologii Informaționale, autoritate administrativă în subordinea MAI*** – pentru domeniul evidențelor poliției cu caracter criminal, contravențional, datele nominale privind persoanele urmărite, dispărute fără veste sau implicate în activități infracționale, date referitoare la vehiculele anunțate în căutare, precum și piesele componente ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, precum și pentru datele dactiloscopice (în partea asigurării funcționării Sistemului informațional automatizat „Registrul de stat dactiloscopic” și a comunicațiilor aferente schimbului de date dactiloscopice);
- ***Inspectoratul General de Carabinieri, autoritate administrativă în subordinea MAI*** – pentru domeniul pentru evenimente majore cu dimensiune transfrontalieră;
- ***Agenția Servicii Publice*** – pentru domeniul de date privind mijloacele de transport, date privind pașapoartele, cărțile de identitate și buletinele de identitate ale cetățeanului Republicii Moldova, inclusiv a celor declarate false, furate sau pierdute, precum și date privind permisele de conducere;
- ***Serviciul de Informații și Securitate al Republicii Moldova*** – pentru domeniul furnizării informațiilor necesare prevenirii infracțiunilor cu caracter terorist, în regim de informații indirect accesibile, în condițiile, limitele și conform procedurilor prevăzute de legislația națională;
- ***Serviciul Tehnologia Informației și Securitate Cibernetică*** – în calitate de punct național de conectare la domeniul local la rețeaua de comunicații securizată a Uniunii Europene TESTA, responsabil de asigurarea conectivității, funcționării, disponibilității și securității canalului național de comunicații utilizat pentru schimbul de date.

Principalele prevederi ale proiectului și evidențierea elementelor noi:

1) Utilizarea **Router-ului UE** ca punct central pentru interogarea automatizată a datelor biometrice, permițând extragerea și evaluarea rapidă a profilurilor ADN, amprentelor și imaginilor faciale.

2) Implementarea sistemului **EPRIS** (Sistemul european de inventariere a evidențelor poliției), care permite verificarea existenței unor antecedente sau evidențe polițienești în alte state membre, folosind date pseudonimizate pentru protecția identității în etapa de căutare.

3) Proiectul de hotărârii de Guvern reglementează obligativitatea utilizării standardului **UMF (Universal Message Format)** pentru toate mesajele structurate, garantând astfel interoperabilitatea tehnică între sistemele naționale și cele europene.

4) Sunt stabilite unele termene limită pentru furnizarea informațiilor solicitate, menite să asigure operativitatea urmăririi penale: **8 ore** pentru cereri urgente (date direct accesibile), **3 zile** pentru cereri urgente (date indirect accesibile) și **7 zile** pentru restul solicitărilor.

5) Introducerea procedurii de **revizuire manuală obligatorie** de către un expert calificat pentru orice concordanță (hit) biometrică înainte de a confirma rezultatul către statul solicitant.

6) Reglementarea „setului de date de bază” care se returnează automatizat în 48 de ore după confirmarea manuală a unei concordanțe, facilitând identificarea rapidă a persoanelor implicate în infracțiuni grave.

7) Instituirea unui mecanism anual de raportare către Comisia Europeană, cuprinzând statistici detaliate privind volumul de cereri, ratele de concordanță (hits) și motivele de refuz, în scopul evaluării eficienței cooperării transfrontaliere.

Proiectul instituie o separare riguroasă între datele biometrice administrative și cele criminogene. Datele biometrice colectate de Agenția Servicii Publice exclusiv pentru verificarea autenticității actelor de identitate și a identității titularului, care fac obiectul ștergerii automate conform HG nr. 125/2013, nu sunt utilizate în mecanismul de căutare automatizată. Interfața tehnică gestionată de ASP vizează exclusiv statutul juridic al documentului (validitate, furt, pierdere) și nu permite, din punct de vedere tehnic, accesul la datele biometrice stocate pe mediul electronic al documentului. Schimbul de date biometrice (ADN, amprente) vizează exclusiv bazele de date gestionate de STI și CTCEJ, constituite în scopul prevenirii și investigării infracțiunilor.

Deși Direcția Cooperare Polițienească Internațională a Inspectoratului General al Poliției exercită rolul punctului unic de contact și gestionează fluxurile de informații prin intermediul INTERPOL, Europol (aplicația SIENA) și ofițerii de legătură, nu există un cadru normativ național care să definească clar structura, funcționarea 24/7 și competențele Punctului unic de contact conform noilor cerințe europene (inclusiv accesul direct la toate bazele de date naționale relevante).

Informațiile sunt deținute de autorități diferite (Poliție, Centrul Național Anticorupție, Serviciul Vamal, Poliția de Frontieră), iar schimbul între acestea și partenerii străini nu este întotdeauna centralizat prin canale securizate unice, ceea ce duce la întârzieri.

Intervenția normativă vizează instituționalizarea Punctului de Contact Unic, stabilirea SIENA ca instrument principal de comunicare și impunerea unor termene de răspuns stricte. Aceasta va asigura că Republica Moldova nu rămâne un "punct orb" în arhitectura de securitate a UE, facilitând totodată parcursul de aderare prin alinierea la standardele capitolului 24 (Justiție, Libertate și Securitate).

Un element central al proiectului este instituirea mecanismului de aplicare eșalonată a prevederilor ce vizează interconectarea cu infrastructurile centrale ale Uniunii Europene (Router-ul UE, EPRIS, EUCARIS, Sistemul de Informații Schengen/SIRENE etc.). Având în vedere statutul de stat candidat al Republicii Moldova, proiectul introduce o clauză expresă de aplicare condiționată, care stipulează că normele operative ce implică accesul direct la sistemele securizate ale UE nu produc efecte juridice și tehnice depline de la data adoptării.

Acestea urmează a fi puse în aplicare progresiv, pe măsura asigurării condițiilor tehnice și juridice necesare, după obținerea dreptului de acces la mecanismele respective în temeiul tratatelor internaționale sau de la data aderării la Uniunea Europeană. Acest demers previne crearea unei aparențe de aplicabilitate imediată a unor mecanisme la care Republica Moldova nu are încă acces deplin, asigurând totodată cadrul normativ necesar pentru pregătirea tehnică internă. Până la obținerea acestui acces, schimbul de date se va realiza prin utilizarea canalelor de cooperare internațională deja disponibile, precum Interpol sau SELEC, în măsura compatibilității cu procedurile de triaj stabilite.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

Menținerea situației actuale (nereglementarea) ar menține riscurile de securitate și ar izola Republica Moldova de mecanismele europene de cooperare polițienească automatizată.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Impactul asupra sectorului public este unul preponderent instituțional, normativ și tehnico-organizațional. În mod direct, autoritățile publice cu atribuții în domeniul ordinii publice și al cooperării polițienești vor trebui să instituie și să aplice proceduri unitare pentru căutarea automatizată și schimbul standardizat de informații, în condițiile stabilite de lege și de reglementările

ulterioare.

Sectorul public va beneficia de o actualizare tehnologică semnificativă prin adoptarea standardului european **UMF (Universal Message Format)** și conectarea la **Router-ul UE**. Această aliniere tehnologică nu doar că facilitează schimbul de date cu statele membre UE, dar impune și la nivel național o mai bună structurare și digitalizare a bazelor de date deținute de IGP, STI, ASP și SIS, eliminând fragmentarea informațională.

Proiectul impune autorităților publice mecanisme stricte monitorizare și verificare a accesului la date. Acest lucru va consolida responsabilitatea funcționarilor publici și va asigura un nivel înalt de protecție a drepturilor cetățenilor, conform standardelor europene, reducând riscul de acces neautorizat sau utilizare abuzivă a informațiilor sensibile.

Autoritățile desemnate ca PNC vor trebui să asigure interoperabilitatea sistemelor proprii cu nodurile de comunicații ale PUC.

4.2. Impactul financiar și argumentarea costurilor estimative

Aprobarea prezentului proiect de hotărâre nu generează cheltuieli suplimentare imediate de la bugetul de stat și nu impune noi responsabilități administrative exclusive Ministerului Afacerilor Interne. Implementarea acestuia se bazează pe un efort instituțional comun de optimizare a infrastructurii tehnice și a canalelor de cooperare deținute de toate autoritățile implicate, desemnate în calitate de Puncte Naționale de Contact (PNC).

La etapa actuală, proiectul hotărârii Guvernului instituie cadrul normativ general și nu stabilește alocări bugetare sau obligații financiare imediate exprimate în sume fixe. Costurile efective vor fi determinate eșalonat, pe măsura elaborării documentației tehnice și a specificațiilor funcționale pentru interconectarea cu Router-ul UE, sistemul EPRIS și EUCARIS. Punerea acestora în aplicare este condiționată de obținerea accesului juridic și tehnic în temeiul tratatelor internaționale sau de la data aderării Republicii Moldova la UE, ceea ce permite o planificare financiară strategică pe termen mediu și lung, evitând presiunea asupra bugetului curent.

Activitățile necesare pentru implementarea sistemelor de schimb de date vor viza, în principal:

- dezvoltarea interfețelor tehnice pentru interconectarea registrelor naționale de referință (ADN, dactiloscopie, vehicule) cu infrastructura europeană, sarcină ce revine fiecărei autorități deținătoare de date (PNC);
- implementarea standardului UMF pentru asigurarea interoperabilității automate, activitate realizată în cadrul modernizării curente a sistemelor proprii ale PNC;
- asigurarea conectivității securizate prin rețeaua TESTA, administrată tehnic de către STISC;
- instruirea personalului calificat pentru revizuirea manuală a concordanțelor biometrice, proces ce va fi susținut prioritar prin programe de asistență externă și suport tehnic oferit de agențiile UE (Europol, eu-LISA);
- mentenanța operativă 24/7 a fluxurilor de date, asigurată prin optimizarea schemelor de serviciu existente în cadrul subdiviziunilor specializate ale PNC și PUC (ex: Secția 24/7 a DCPI), fără a genera costuri administrative noi de personal.

Sustenabilitatea financiară a proiectului este garantată prin utilizarea infrastructurii naționale de interoperabilitate MConnect și a canalelor internaționale deja operabile (SIENA, Interpol), care nu necesită investiții suplimentare pentru faza de lansare. Mai mult, procesul de aliniere tehnică la standardele UE este planificat și bugetat în cadrul Consiliului de Coordonare pentru Conectarea la Ecosistemul eu-LISA (instituit prin Ordinul Comun din 30.03.2026), cheltuielile fiind acoperite descentralizat de cele 19 instituții membre. Implementarea componentelor costisitoare (precum Router-ul UE) este eșalonată și condiționată de obținerea accesului juridic la nivel de Uniune Europeană, conform clauzei de intrare în vigoare a prezentului proiect.

Finanțarea măsurilor de implementare va fi realizată în limita alocațiilor aprobate Ministerului Afacerilor Interne și instituțiilor din subordine (Inspectoratul General al Poliției, Serviciul Tehnologii Informaționale al MAI, Inspectoratul General de Carabinieri al MAI), autorităților desemnate în calitate de PNC (Agenția Servicii Publice, Serviciul de Informații și Securitate), precum și, după caz, din alte surse legal disponibile, inclusiv proiecte de asistență externă, programe de suport tehnic sau alte mecanisme financiare aferente procesului de modernizare instituțională și integrare europeană.

Astfel, proiectul nu instituie cheltuieli imediate prin aprobarea prezentului proiect de hotărâre, însă creează cadrul normativ care va permite planificarea etapizată a resurselor financiare necesare

pentru facilitarea schimbului de date în domeniul cooperării polițienești transfrontaliere. Costurile vor fi justificate prin necesitatea instituirii unei resurse informaționale specializate de stat (Sistemul electronic unic de gestionare a cazurilor), capabilă să asigure triajul, evidența, monitorizarea și trasabilitatea tuturor operațiunilor de acces și schimb de date, garantând interoperabilitatea tehnică cu infrastructura Uniunii Europene.

În ceea ce privește implicarea instanțelor, examinarea cererilor de autorizare judiciară se va realiza prin mecanismele de permanență (24/7) deja instituite prin actele Consiliului Superior al Magistraturii, asigurându-se un tratament nediscriminatoriu al cererilor fără costuri suplimentare de personal.

4.3. Impactul asupra sectorului privat

Proiectul nu instituie obligații directe de raportare sau conformare pentru sectorul privat, întrucât se aplică autorităților competente și privește mecanismele de cooperare polițienească transfrontalieră și schimbul de date în scopuri de aplicare a legii. Prin urmare, nu se anticipează costuri administrative sau de conformare pentru întreprinderi, profesioniști ori alte entități private, în sensul impunerii de noi proceduri, licențe, autorizări sau raportări periodice.

Impactul indirect asupra sectorului privat este preponderent pozitiv și rezultă din consolidarea capacității de prevenire și investigare a criminalității transfrontaliere, cu efecte asupra reducerii riscurilor economice asociate fraudei, furturilor de vehicule, falsurilor, criminalității organizate și altor forme de infracționalitate care afectează mediul de afaceri. De asemenea, creșterea eficienței schimbului de informații poate conduce la scurtarea duratei investigațiilor în cauze cu element transfrontalier și la îmbunătățirea recuperării bunurilor, ceea ce reduce pierderile suportate de agenții economici și de asigurători.

Schimbul automatizat de date privind înmatricularea vehiculelor și permisele de conducere permite o soluționare mult mai rapidă a cazurilor de furt de vehicule sau a accidentelor rutiere implicând autoturisme înmatriculate în străinătate.

4.4. Impactul social

Proiectul are un impact social preponderent pozitiv, prin creșterea capacității autorităților competente de a preveni, depista și investiga infracțiunile cu componentă transfrontalieră și de a răspunde mai rapid la riscuri de securitate, inclusiv în contextul evenimentelor majore. Accelerarea schimbului de informații și utilizarea căutărilor automatizate pot reduce timpul de identificare a persoanelor și de confirmare a concordanțelor între date, contribuind la sporirea siguranței publice și a securității.

Principalul beneficiu social este descurajarea criminalității și creșterea sentimentului de siguranță în rândul cetățenilor. Prin eficientizarea schimbului de date (ADN, amprente, imagini faciale), probabilitatea ca autorii infracțiunilor grave să fie identificați și trași la răspundere crește considerabil. Acest lucru reduce riscul de victimizare a populației și contribuie la un mediu social mai stabil.

Modernizarea mecanismelor de cooperare polițienească demonstrează capacitatea statului de a proteja ordinea publică folosind tehnologii de ultimă generație. Transparența și rigoarea procedurilor europene implementate prin acest proiect vor spori încrederea cetățenilor în profesionalismul și eficiența autorităților de aplicare a legii.

4.4.1. Impactul asupra datelor cu caracter personal

Proiectul are un impact direct și semnificativ asupra prelucrării datelor cu caracter personal, instituind cadrul juridic necesar pentru schimbul automatizat de informații sensibile, precum profilurile ADN, datele dactiloscopice și imaginile faciale, precum și a evidențelor polițienești. Întreaga arhitectură a schimbului de date este proiectată să asigure respectarea riguroasă a Legii nr. 195/2024 privind protecția datelor cu caracter personal, care constituie pilonul central de referință pentru toate operațiunile de procesare efectuate de Punctul Unic de Contact (PUC) și Punctele Naționale de Contact (PNC).

Se introduce un regim diferențiat de jurnalizare (log-uri), adaptat cerințelor tehnice și de securitate ale infrastructurilor europene. Astfel, în timp ce pentru operațiunile generale de schimb de date se menține termenul de păstrare a înregistrărilor de 3 ani, pentru toate căutările și interogările automatizate realizate prin intermediul Router-ului UE, al Portalului European de Căutare (ESP) sau al Depozitului Comun de Date de Identitate (CIR), înregistrările se vor păstra pentru o perioadă de

minimum 5 ani. Această extindere a termenului asigură o pistă de audit nealterabilă și conformă cu standardele europene de interoperabilitate, permițând monitorizarea riguroasă a legalității prelucrării datelor biometrice și a imaginilor faciale.

Impactul este unul de securizare și responsabilizare, ridicând nivelul de protecție a datelor la standardele Uniunii Europene (Regulamentul Prüm II și Directiva 2023/977). Pentru a garanta drepturile persoanelor vizate, proiectul instituie următoarele mecanisme de salvgardare conform Legii nr. 195/2024:

- **Respectarea principiilor de bază**: Prelucrarea este strict limitată la scopurile determinate de prevenire și investigare a infracțiunilor, fiind guvernată de principiile necesității, proporționalității și minimizării datelor;
- **Intervenția umană obligatorie**: Orice concordanță (hit) rezultată în urma interogărilor automatizate a datelor biometrice este supusă unei revizuiri manuale obligatorii de către un expert calificat, eliminând riscul unor decizii bazate exclusiv pe procese automatizate;
- **Trasabilitate și control**: Se instituie obligația de jurnalizare (log-uri) a tuturor operațiunilor de acces și schimb de date pentru o perioadă de 3 ani, asigurând astfel o pistă de audit nealterabilă pentru verificările efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal (CNPDCP);
- **Drepturile persoanei vizate**: Proiectul reglementează proceduri clare pentru exercitarea dreptului de acces, rectificare și ștergere a datelor, inclusiv instituirea mecanismului de marcare a datelor contestate pentru a limita utilizarea acestora până la clarificarea situației;
- **Securitate tehnică avansată**: Schimbul de date se realizează prin canale criptate (rețeaua TESTA) și interfețe securizate (SIENA, MConnect), cu aplicarea autentificării multifactoriale și raportarea obligatorie a incidentelor de securitate către CERT-UE în termen de 24 de ore.

Prin aceste măsuri, proiectul asigură un echilibru corect între necesitatea operativă a autorităților de aplicare a legii și protecția drepturilor fundamentale ale cetățenilor, sub supravegherea permanentă a CNPDCP.

4.4.2. Impactul asupra echității și egalității de gen

Nu este aplicabil.

4.5. Impactul asupra mediului

Nu este aplicabil.

4.6. Alte impacturi și informații relevante

Nu este aplicabil.

5. Compatibilitatea proiectului actului normativ cu legislația UE

5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională

Proiectul transpune parțial următoarele acte juridice ale Uniunii Europene:

✓ Regulamentul (UE) 2024/982 Parlamentului European și al Consiliului din 13 martie 2024 privind căutarea și schimbul automatizat de date în scopul cooperării polițienești, și de modificare a Deciziilor 2008/615/JAI și 2008/616/JAI ale Consiliului și a Regulamentelor (UE) 2018/1726, (UE) 2019/817 și (UE) 2019/818 ale Parlamentului European și ale Consiliului (Regulamentul Prüm II), publicat în Jurnalul Oficial al Uniunii Europene L 2024/982 din 5 aprilie 2024, CELEX: 32024R0982;

✓ Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere, publicată în Jurnalul Oficial al Uniunii Europene, L 210 din 6 august 2008, așa cum a fost modificată ultima oară prin Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024, CELEX: 32008D0615;

✓ Decizia 2008/616/JAI a Consiliului din 23 iunie 2008 privind punerea în aplicare a Deciziei 2008/615/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere, publicată în Jurnalul Oficial al Uniunii Europene, L 210/12 din 6 august 2008, așa cum a fost modificată ultima oară prin Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024, CELEX: 02008D0616-20240425;

✓ Directiva (UE) 2023/977 a Parlamentului European și a Consiliului din 10 mai 2023 privind schimbul de informații dintre autoritățile de aplicare a legii ale statelor membre și de abrogare a Deciziei-cadru 2006/960/JAI a Consiliului, publicată în Jurnalul Oficial al Uniunii Europene, L 134/1 din 22 mai 2023, CELEX: 32023L0977;

✓ Decizia 2004/919/CE a Consiliului din 22 decembrie 2004 privind combaterea criminalității referitoare la vehicule și având implicații transfrontaliere, publicată în Jurnalul Oficial al Uniunii Europene, L 389/28 din 30 decembrie 2004, CELEX: 32004D0919.

Proiectul realizează transpunerea normelor Uniunii Europene într-o manieră consolidată, raportându-se exclusiv la prevederile în vigoare ale acquis-ului Prüm. Astfel, transpunerea Deciziilor 2008/615/JAI și 2008/616/JAI este limitată strict la acele articole care produc în prezent efecte juridice și care nu au fost absorbite sau înlocuite de noile mecanisme tehnice și procedurale instituite prin Regulamentul (UE) 2024/982 (Prüm II). Această abordare asigură o corelare exactă între normele de cooperare operativă (Decizia 615), procedurile tehnice de punere în aplicare (Decizia 616) și noile standarde de interoperabilitate europene.

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

Proiectul depășește simpla desemnare instituțională, instituind un mecanism complex de implementare a acquis-ului UE prin următoarele măsuri normative concrete:

1. **Instituționalizarea Punctului Unic de Contact:** Proiectul creează structura administrativă și operațională necesară pentru a asigura un flux informațional securizat și centralizat 24/7 între autoritățile naționale și partenerii internaționali, eliminând fragmentarea actuală a canalelor de comunicare;

2. **Operaționalizarea Punctelor Naționale de Contact pe domenii de specialitate:** Sunt stabilite atribuții clare și competențe tehnice exclusive pentru autoritățile deținătoare de date (Inspectoratul General al Poliției, Serviciul Tehnologii Informaționale al MAI, Agenția Servicii Publice, Serviciul de Informații și Securitate), asigurând astfel „nodurile" naționale necesare pentru interconectarea la infrastructurile biometrice (Router-ul UE), de evidențe polițienești (EPRIS) și auto (EUCARIS);

3. **Implementarea standardelor tehnice de interoperabilitate:** Se impune utilizarea obligatorie a standardului UMF (Universal Message Format) și a rețelei securizate TESTA, măsuri care garantează că sistemele informatice naționale pot „comunica" automatizat cu cele ale statelor membre UE, asigurând tranzitul securizat al datelor;

4. **Reglementarea procedurilor de eficiență operativă:** Proiectul introduce termene stricte de furnizare a informațiilor (8 ore, 3 zile sau 7 zile), mecanisme de triaj automatizat pentru prevenirea suprapunerii investigațiilor și proceduri clare pentru obținerea autorizațiilor judiciare necesare schimburilor internaționale, conform standardelor Directivei 2023/977;

5. **Implementarea principiului „Digital by Default" prin platforma MConnect:** Proiectul definește platforma guvernamentală de interoperabilitate MConnect ca stratul principal de interconectare națională, prin care Punctele Naționale de Contact (PNC) au obligația de a asigura furnizarea datelor către Sistemul electronic unic de gestionare a cazurilor administrat de PUC. Această măsură elimină necesitatea unor conexiuni punct-la-punct fragmentate și asigură un tranzit securizat și automatizat al informațiilor din registrele de stat către interfețele tehnice internaționale.

6. **Reglementarea fluxului operativ pentru alertele Sistemului de Informații Schengen:** Se stabilesc atribuții specifice pentru Agenția Servicii Publice (ASP) de a asigura interfața tehnică și fluxul de date necesar pentru introducerea imediată în Sistemul de Informații Schengen (SIS) a alertelor referitoare la mijloacele de transport și documente (pașapoarte, certificate de înmatriculare și permise de conducere) raportate ca fiind furate, pierdute, sustrase sau anulate;

7. **Coordonarea prin Biroul Național SIRENE:** Proiectul standardizează interacțiunea dintre ASP și Biroul Național SIRENE din cadrul PUC, impunând transmiterea fără întârziere a informațiilor pentru gestionarea operativă a alertelor, garantând astfel că Republica Moldova contribuie activ la securitatea spațiului european prin raportarea bunurilor și documentelor urmărite internațional;

8. **Delimitarea accesului la datele biometrice administrative:** Se precizează clar că interfața gestionată de ASP pentru verificarea documentelor vizează exclusiv statutul juridic al documentului și nu permite accesul tehnic la datele biometrice stocate pe mediul electronic al acestuia, asigurând un cadru riguros de protecție a datelor în raport cu funcționalitățile Sistemului de Informații Schengen și SLTD (Interpol);

9. **Cadrul de protecție și control al datelor:** Proiectul operaționalizează cerințele de protecție a datelor prin instituirea revizuirii manuale obligatorii a concordanțelor biometrice, a procedurii de marcare a datelor contestate și a obligației de jurnalizare (log-uri) a tuturor operațiunilor pentru o perioadă de 3 ani, facilitând auditul extern efectuat de CNPDCP;

10. **Eșalonarea implementării tehnice:** Se stabilește o clauză de punere în aplicare progresivă, condiționată de asigurarea pregătirii tehnice și obținerea accesului juridic la sistemele UE, asigurând astfel o tranziție predictibilă către standardele de aderare.

6. Avizarea și consultarea publică a proiectului

În vederea respectării prevederilor Legii nr. 100/2017 cu privire la actele normative și ale Legii nr. 239/2008 privind transparența în procesul decizional, anunțul privind inițierea elaborării prezentului proiect a fost plasat pe platforma guvernamentală www.particip.gov.md.

Totodată, proiectul de hotărâre de Guvern a fost supus procesului de consultare publică, fiind plasat pe pagina web oficială a Ministerului Afacerilor Interne, la compartimentul „Transparența”, rubrica „Consultări publice”, precum și pe platforma guvernamentală www.particip.gov.md, fiind disponibil la link-ul.

În cadrul procesului de consultare, părțile interesate au avut posibilitatea de a transmite propuneri și recomandări. Rezultatele acestui proces, precum și analiza obiecțiilor recepționate de la autoritățile avizatoare (Ministerul Justiției, Ministerul Afacerilor Externe, Serviciul de Informații și Securitate, Agenția Servicii Publice și alte instituții relevante), sunt reflectate în Sinteza obiecțiilor, care constituie parte integrantă a dosarului de însoțire a proiectului.

La data de 06.08.2026, proiectul hotărârii de Guvern a fost transmis Comisiei Europene pentru consultări. La 28.09.2026 au fost recepționate comentariile formulate de Comisia Europeană. Toate recomandările înaintate pe marginea proiectului au fost incluse în Tabelul de sinteza.

7. Concluziile expertizelor

Proiectul a fost supus expertizei de compatibilitate cu legislația UE de către Centrul de Armonizare a Legislației, fiind obținut avizul de compatibilitate, acesta fiind inclus în tabelul de sinteză a obiecțiilor. Totodată, proiectul a fost supus expertizei anticorupție și expertizei juridice în conformitate cu art. 35 și 36 din Legea nr. 100/2017, concluziile au fost incorporate în Tabelul de sinteză a obiecțiilor și propunerilor.

8. Modul de încorporare a actului în cadrul normativ existent

Proiectul elaborat se încadrează în cadrul normativ, iar adoptarea proiectului nu impune modificarea sau abrogarea a careva acte normative.

Pe perioada de tranziție, până la activarea accesului la mecanismele Uniunii Europene, schimbul de date se va realiza prin utilizarea canalelor de cooperare internațională deja disponibile, precum Interpol, SELEC și acordurile bilaterale. Procedurile de triaj, validare manuală a concordanțelor biometrice și management al cazurilor prevăzute în regulamentele anexate vor fi aplicate în măsura compatibilității cu aceste sisteme existente, asigurând o tranziție lină către standardele de lucru europene.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

După elaborarea și aprobarea proiectului de lege și a hotărârilor de Guvern menționate supra, vor fi modificare fișele de post și Regulamentele de activitate ale subdiviziunilor/autorităților din cadrul cărora vor fi desemnate puncte de contact pentru schimbului de date și informațiicu statele membre.

În vederea asigurării transpunerii depline a specificațiilor tehnice și operaționale detaliate din Anexa la Decizia 2008/616/JAI (referitoare la formatele de date ADN, standardele de calitate dactiloscopice și protocoalele de comunicare pentru datele vehiculelor), implementarea proiectului va include aprobarea unui ordin interinstituțional între autoritățile desemnate în calitate de PNC și PUC. Această măsură va permite alinierea eșalonată și flexibilă a infrastructurii naționale la

standardele tehnice de interoperabilitate ale Uniunii Europene (Prüm II), pe măsura obținerii accesului juridic și tehnic la Router-ul UE, EPRIS și EUCARIS.

Suplimentar acțiunilor de modificare a cadrului normativ intern, implementarea proiectului necesită realizarea unui program complex de instruire, structurat pe două paliere:

1. *Instruirea operativă și tehnică:* Personalul desemnat în cadrul PUC și PNC va beneficia de formare specializată privind utilizarea standardului UMF, a aplicației SIENA și a infrastructurilor Router UE și EPRIS. Acest proces va fi coordonat prin intermediul Consiliului de Coordonare pentru Conectarea la Ecosistemul eu-LISA, care are atribuția expresă de a sprijini organizarea programelor de formare și dezvoltare a capacităților instituționale.

2. *Formarea specializată a magistraților*: Având în vedere mecanismele de autorizare judiciară prevăzute în Anexa nr. 1, Ministerul Afacerilor Interne va colabora cu Institutul Național al Justiției pentru includerea în programele de formare inițială și continuă a procurorilor și judecătorilor a unor module specifice privind cooperarea polițienească internațională, standardele de protecție a datelor biometrice și procedurile de urgență pentru schimbul de informații conform acquis-ului UE.

De asemenea, se va asigura participarea personalului relevant la programele de instruire oferite de agențiile Uniunii Europene (Europol, CEPOL și eu-LISA), utilizând inclusiv materialele informaționale și studiile puse la dispoziție prin rețeaua acestora.

Având în vedere complexitatea mecanismelor de autorizare judiciară a schimburilor de date biometrice și necesitatea respectării termenelor de urgență (8 ore/3 zile), Ministerul Afacerilor Interne va stabili un parteneriat strategic cu Institutul Național al Justiției. Acesta va viza includerea în programele de formare inițială și continuă a judecătorilor și procurorilor a unor module dedicate cooperării polițienești internaționale, cu accent pe standardele de protecție a datelor biometrice, procedurile de urgență conform acquis-ului Prüm II și funcționarea mecanismelor de permanență (24/7) pentru autorizarea judiciară.

Procesul de instruire operativă și tehnică a personalului desemnat în cadrul PUC și al Punctelor Naționale de Contact va fi coordonat prin intermediul Consiliului de Coordonare pentru Conectarea la Ecosistemul eu-LISA. Acest consiliu va asigura planificarea sesiunilor de formare pentru utilizarea standardului UMF, a aplicației SIENA și a infrastructurilor Router UE și EPRIS, facilitând totodată accesul experților naționali la programele de asistență tehnică și instruire oferite de agențiile Uniunii Europene (Europol, eu-LISA și CEPOL).

Secretar de stat **Victor GROSU**

SINTEZA
obiecțiilor și propunerilor (recomandărilor)
la proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact
și a Punctelor Naționale de Contact în scopul schimbului automatizat de date

Participantul la avizare (expertizare)/consultare publică		**Conținutul obiecției/ propunerii (recomandării)**	**Argumentarea autorului proiectului**
AVIZARE ȘI CONSULTARE PUBLICĂ			
Agenția Servicii Publice (nr. 01/5357 din 09.06.2026)	**1**	La pct. 1.4 din proiectul hotărârii Guvernului, precum și la pct. 4.4 și 62 din Anexa nr. 2 „Regulamentul de organizare și funcționare a Punctelor Naționale de Contact în scopul schimbului de date și informații”: • **„autovehiculele anunțate în căutare și piesele urmărite internațional”:** Acestea constituie obiectul de evidență al „Registrului informației criminalistice și criminologice”, deținut de Ministerul Afacerilor Interne, conform Hotărârii Guvernului nr. 633/2007 cu privire la aprobarea Concepției Sistemului informațional automatizat „Registrul informației criminalistice și criminologice”.	**Se acceptă** Proiect ajustat, prin: - modificarea subpct. 1.2. și subpct . 1.4. din partea dispozitivă a proiectului hotărârii de Guvern; - modificarea subpct . 4.2. și subpct . 4.4. din Anexa nr. 2 a proiectului hotărârii de Guvern; - modificarea pct. 48. din Anexa nr. 2 a proiectului hotărârii de Guvern; - modificarea pct. 62. din Anexa nr. 2 a proiectului hotărârii de Guvern.
	2	• **„date privind documentele de călătorie”:** ASP poate furniza date despre pașapoartele, cărțile de identitate și buletinele de identitate ale cetățeanului Republicii Moldova. În acest sens, se solicită o delimitare a documentelor de călătorie pentru străini eliberate de Inspectoratul General pentru Migrație și cele diplomatice și de serviciu, eliberate de Ministerul Afacerilor Externe. Menționăm că noțiunea „document de călătorie” include mai multe categorii de documente, emise de autorități publice diferite, și anume: a) documentele de călătorie pentru persoanele cărora li s-a recunoscut statutul de apatrid sau de refugiat, precum și pentru persoanele cărora li s-a acordat protecție umanitară, eliberate de Inspectoratul General pentru Migrație; b) pașapoartele diplomatice și pașapoartele de serviciu, eliberate de Ministerul Afacerilor Externe, în condițiile legii, persoanelor care dețin, exclusiv cetățenia Republicii Moldova pentru ieșire și intrare în Republica	**Se acceptă** Proiect ajustat pentru delimitarea categoriilor de documente de călătorie și desemnarea PNC pentru fiecare categorie, prin: - modificarea subpct. 1.4. din partea dispozitivă a proiectului hotărârii de Guvern; - modificarea subpct. 4.4. din Anexa nr. 2 a proiectului hotărârii de Guvern; - modificarea pct. 62., pct. 64. și pct. 65. din Anexa nr. 2 a proiectului hotărârii de Guvern.

		Moldova în vederea îndeplinirii unor misiuni diplomatice și consulare sau unor funcții de serviciu peste hotare.	
	3	• **„vizele”:** Aceste date sunt gestionate, exclusiv prin Sistemul Informațional de Gestionare a Vizelor (SIGV), utilizat de misiunile diplomatice și oficiile consulare din cadrul Ministerului Afacerilor Externe.	**Se acceptă** Proiect ajustat, prin: - modificarea subpct. 1.4. din partea dispozitivă a proiectului hotărârii de Guvern (excluderea cuvântului „vizele”); - modificarea pct. subpct. 4.4. din Anexa nr. 2 a proiectului hotărârii de Guvern (excluderea cuvântului „vizele”); - modificarea pct. 62. din Anexa nr. 2 a proiectului hotărârii de Guvern (excluderea cuvântului „vizele”).
	4	• **„titlurile de valoare (inclusiv cele false/furate/pierdute)”:** Evidența centralizată a acestora este asigurată de Comisia Națională a Pieței Financiare (CNPF) prin „Registrul emitenților de valori mobiliare”, în temeiul Legii nr.234/2016 cu privire la Depozitarul central unic al valorilor mobiliare și a Legii nr.192/1998 privind Comisia Națională a Pieței Financiare. Menținerea acestor categorii în sarcina ASP contravine Statutului Agenției (Hotărârea Guvernului nr. 314/2017) și cadrului normativ aferent registrelor deținute, impunând instituției atribuții pentru care nu deține calitatea de furnizor primar de date. În acest context, documentul urmează să fie revizuit cu redistribuirea responsabilităților conform competențelor deținute de autoritățile de stat.	**Se acceptă** Proiect ajustat, prin: - modificarea subpct. 1.4. din partea dispozitivă a proiectului hotărârii de Guvern (excluderea cuvintelor „titlurile de valoare”); - modificarea subpct. 4.4. din Anexa nr. 2 a proiectului hotărârii de Guvern (excluderea cuvintelor „titlurile de valoare”); - modificarea pct. 62. din Anexa nr. 2 a proiectului hotărârii de Guvern (excluderea cuvintelor „titlurile de valoare”).
	5	La proiectul Regulamentului de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații, care se regăsește în Anexa 1: - la pct. 94, subpct. 94.6. după cuvântul „statutul”, de completat cu cuvântul „procesual”, în contextul în care statutul poate fi de mai multe tipuri, spre exemplu: civil, juridic, etc.; - la pct. 67 potrivit căruia „ASP are obligația de a asigura exactitatea și actualizarea permanentă a datelor din registrele naționale procedând la rectificarea sau ștergerea imediată a informațiilor incorecte ori neactuale identificate în cursul schimbului de date.”, propunem după cuvântul „registrele” de completat cu cuvintele „de stat aflate în posesie”, iar	**Se acceptă** Proiect ajustat prin modificarea subpct. 95.6 din Anexa nr. 1 și pct. 68 din Anexa nr. 2 a proiectului hotărârii de Guvern.

		cuvântul ,,naționale” de substituit cu ,,de stat”, în vederea corelării cu prevederile Legii nr. 71/2007 cu privire la registre și în limita registrelor de stat administrate de ASP, în calitate de posesor, atribuită prin legi speciale și hotărâri de Guvern.	
	6	În nota de fundamentare la proiect, precum si în textul proiectului hotărârii se menționează despre ,,anumite date privind înmatricularea vehiculelor, imagini faciale, biometrie”. Consideram imperios de a specifica datele de acest tip, ce vor fi colectate, stocate (cu indicarea termenului de păstrare) și transmise către terți, pentru o precizie juridică a actului normativ și o delimitare clară a responsabilităților între autorități. Este de menționat, că actualmente ASP asigură prelevarea datelor biometrice ale persoanei fizice, inclusiv amprentele digitale, în conformitate cu prevederile art. 2 alin. (6) și art. 3 alin. (6) din Legea nr. 273/1994 privind actele de identitate din sistemul național de pașapoarte, precum și prevederile pct. 78, 79, 791 din „Regulamentul privind eliberarea actelor de identitate și evidența locuitorilor Republicii Moldova”, aprobat prin Hotărârea Guvernului nr. 125/2013, prevederi care au transpus acquis-ul UE în materie de documente de călătorie: Regulamentul (CE) nr.2252/2004 din 13 decembrie 2004 privind standardele pentru elementele de securitate și elementele biometrice integrate în pașapoarte și documente de călătorie emise de statele membre și Regulamentul UE 2025/1208 al Consiliului din 12 iunie 2025 privind consolidarea securității cărților de identitate ale cetățenilor Uniunii și a documentelor de ședere eliberate cetățenilor Uniunii și membrilor de familie ai acestora care își exercită dreptul la libera circulație. Procedura de stocare și securizare a datelor biometrice este realizată pe plan național, în conformitate cu prevederile internaționale Doc 9303 OACI, Anexele 3, 9, 10, 11 și 12 și anume în procesul de personalizare a actelor de identitate (pașapoarte, documente de călătorie, cărți de identitate, cărți de rezidență), amprentele digitale, de comun cu imaginea facială ale titularului sunt înscrise în mediul de stocare electronică a documentului. Datele biometrice (imaginea facială, imaginile amprentelor digitale) se colectează pentru a fi incluse în cartea de identitate, în cartea de rezidență, în pașaportul și în documentul de călătorie, exclusiv în scopul verificării autenticității acestor acte de identitate și a identității titularului și nu în scopuri criminogene.	**Se acceptă** Proiect ajustat, prin: - modificarea subpct. 76.2. din Anexa nr. 1 a proiectului hotărârii de; - completarea pct. 65. din Anexa nr. 2 a proiectului hotărârii de Guvern. Nota de fundamentare a fost ajustată pentru a asigura o precizie juridică deplină. S-a stabilit o delimitare clară a responsabilităților: ASP gestionează datele administrative privind vehiculele și documentele (furnizate prin EUCARIS/SLTD), în timp ce CTCEJ și STI gestionează datele biometrice și polițienești în scopuri criminalistice (furnizate prin Router/EPRIS). De asemenea Nota de fundamentare a fost completată la Secțiunea 3.1 și Secțiunea 4.4.1 cu următoarele precizări 1. S-a stipulat explicit separarea riguroasă între biometria administrativă (gestionată de ASP conform HG nr. 125/2013) și biometria criminogenă (gestionată de STI și CTCEJ), menționându-se că datele colectate pentru actele de identitate sunt excluse din mecanismele de căutare automatizată. 2. S-a precizat că interfața tehnică a ASP vizează exclusiv statutul juridic al documentului (validitate, furt,

		Totodată, potrivit pct. 791 din Regulamentul privind eliberarea actelor de identitate și evidența locuitorilor Republicii Moldova, aprobat prin Hotărârea Guvernului nr. 125/2013, amprentele digitale prelevate și stocate în resursele informaționale ale ASP se șterg automat, imediat după înmânarea actelor de identitate, iar în cazul în care nu au fost înmânate, cel târziu la împlinirea unui termen de 3 luni de la data personalizării.	pierdere) și, din punct de vedere tehnic, nu permite accesul la datele biometrice stocate pe mediul electronic (cip) al documentului. 3. S-a reconfirmat faptul că proiectul nu afectează regimul de ștergere a datelor biometrice de către ASP, schimbul de date biometrice (ADN, amprente, imagini faciale) vizând exclusiv bazele de date constituite strict în scopul prevenirii și investigării infracțiunilor.
	7	Recomandăm reconfigurarea schimbului de date între sistemele naționale și PUC (Punctul Unic de Contact) prin utilizarea prioritară a platformei guvernamentale de interoperabilitate **MConnect**. Prevederile Legii nr. 142/2018 cu privire la schimbul de date și interoperabilitate și Hotărârea de Guvern nr. 211/2019 privind platforma de interoperabilitate (MConnect) desemnează Agenția de Guvernare Electronică în calitate de autoritate responsabilă de asigurarea tehnică a schimbului de date, inclusiv pentru aspectele ce țin de securitatea informațională și protecția datelor cu caracter personal în tranzit. Solicităm revizuirea Anexei nr. 2 pentru a evita instituirea unor fluxuri de date paralele sau în afara platformei MConnect pentru segmentul național, asigurând astfel respectarea principiului „Digital by Default”.	**Se acceptă** Proiect ajustat prin: - modificarea pct. 5 din Anexa nr. 2 a proiectului hotărârii de Guvern; - modificarea pct. 11 din Anexa nr. 2 a proiectului hotărârii de Guvern; - includerea noului punct 85. în Anexa nr. 2 a proiectului hotărârii de Guvern.
	8	Având în vedere că platforma MConnect dispune deja de mecanisme integrate de jurnalizare a tuturor operațiunilor de acces (log-uri) și de generare a rapoartelor statistice, se solicită ajustarea Anexei nr. 2 la aceste funcționalități existente. Implementarea unor sisteme de jurnalizare redundante la nivel de PNC ar genera sarcini administrative suplimentare nejustificate, în contextul în care trasabilitatea acțiunilor este deja garantată prin infrastructura guvernamentală partajată.	**Se acceptă** Proiect ajustat prin: - modificarea pct. 34., pct. 35. și pct. 36. din Anexa nr. 2 a proiectului hotărârii de Guvern; - includerea noilor puncte în Anexa nr. 2 a proiectului hotărârii de Guvern, și anume: pct. 54., pct. 61., pct. 72. și pct. 85.
Centrul de Armonizare a Legislației (nr. 31/02-126-6416 din 05.06.2026)	**9**	În conformitate cu pct. 24 din Anexa I a proiectului național, prelungirea termenelor se permite în cazuri excepționale, când cererea vizează un volum mare de date și implică mai multe autorități sau verificări complexe. Această soluție trebuie revizuită, deoarece art. 5 (1) din Directiva	**Se acceptă** Proiect ajustat prin:

		(UE) 2023/977 stabilește termene maxime obligatorii, iar derogările trebuie reglementate restrictiv, în special, pentru situațiile care implică autorizație judiciară sau impedimente obiective. Formula actuală este prea largă și poate determina interpretarea relativă a termenelor de 8 ore, 3 zile și 7 zile. La concret, art. 5 (1) din Directiva (UE) 2023/977 fixează termene maxime de 8 ore (informații direct accesibile, în cazuri urgente), 3 zile (informații indirect accesibile, în cazuri urgente) și 7 zile (celelalte cereri). Aceste termene pot fi prelungite numai în ipotezele strict prevăzute de directivă: necesitatea unei autorizații judiciare sau imposibilitatea obiectivă, cu obligația informării fără întârziere a autorității solicitante și a furnizării parțiale a informațiilor disponibile. Astfel, se recomandă reformularea pct. 24 din Anexa nr. 1, prin eliminarea temeiurilor de prelungire neprevăzute de Directivă, precum: „volum mare de date", „verificări transfrontaliere complexe" și limitarea expresă la cazul autorizației judiciare și la situațiile obiective de indisponibilitate, cu păstrarea obligațiilor de comunicare imediată și de furnizare eșalonată a informațiilor.	- modificarea pct. 25., și pct. 26. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	10	Întrucât Decizia 2008/615/JAI a fost amendată substanțial prin Regulamentul (UE) 2024/982, transpunerea acesteia prin proiect urmează a fi raportată exclusiv la prevederile în vigoare. Astfel, Tabelul de concordanță trebuie să identifice expres articolele din Decizia 2008/615/JAI care mai produc efecte și care au fost preluate de cadrul Prüm II, pentru a evita dublarea reglementării și transpunerea unor norme înlocuite/modificate.	**Se acceptă** Tabelul de concordanță a fost revizuit pentru a identifica cu precizie articolele din Deciziile 2008/615/JAI și 2008/616/JAI care sunt transpuse prin prezentul proiect, fiind excluse normele care au fost abrogate sau modificate substanțial prin Regulamentul (UE) 2024/982 (Prüm II). Având în vedere că Decizia 2008/616/JAI reprezintă instrumentul de punere în aplicare a Deciziei 2008/615/JAI, proiectul preia parțial prevederile acestora referitoare la cooperarea în contextul evenimentelor majore și prevenirea terorismului, asigurând totodată alinierea tehnică la noile cerințe de interoperabilitate. Această abordare elimină riscul dublării reglementărilor și garantează că legislația națională reflectă versiunea

			actualizată a acquis-ului UE în domeniul schimbului de date.
	11	Potrivit Tabelului de concordanță, art. 2 lit. h) din Decizia 2008/616/JAI, noțiunea de „**notă**”, este marcat ca **prevedere UE netranspusă**. Justificarea adusă de autorul proiectului este că noțiunea nu a fost preluată pentru a evita paralelismele cu „marcarea datelor”. Totuși, dacă Decizia 2008/616/JAI se menține în lista de transpunere, noțiunea trebuie tratată distinct, deoarece „notă” în sensul deciziei privește marcarea unui profil ADN după obținerea unei concordanțe, iar „marcarea datelor” din proiect are funcție de protecție/limitare a prelucrări.	**Nu se acceptă** Nu a fost preluată terminologic în proiectul HG pentru a evita paralelismele și confuziile cu termenul de „marcare a datelor”, utilizat consecvent pe parcursul textului proiectului HG. De asemenea, precizăm că proiectul de Hotărâre de Guvern și *Legea nr. 209/2026 privind cooperarea polițienească internațională* au fost elaborate în baza versiunilor actualizate ale actelor UE, transpuse prin prisma Regulamentului (UE) 2024/982 (Prüm II), care a modificat substanțial Decizia 2008/616/JAI. În această ordine de idei, menționăm faptul că procedura de marcare a rezultatului pozitiv (fosta „notă”) este acum integrată în „confirmarea concordanței”, care implică revizuirea manuală de către un expert înainte de transmiterea setului de date de bază, conform noțiunii de „concordanță (hit) din Art. 3, prevederilor Art. 11 alin. (7) din Proiectul de Lege și prevederilor aferente cazurilor de concordanță din Proiectul Hotărârii de Guvern.
	12	Analizând proiectul prin prisma prevederilor Deciziei 2008/616/JAI, constatăm că, acesta nu a asigurat transpunerea Anexei din actul UE, iar Tabelul de concordanță nu conține informații referitoare la motivele netranspunerii sau planificarea transpunerii de viitor a acestora. Recomandăm fie transpunerea elementelor relevante din Anexa la Decizia 2008/616/JAI, fie justificarea expresă a netranspunerii în Tabel și, după caz, cu calificarea acestora ca prevederi tehnice aplicabile numai după obținerea accesului la infrastructurile UE.	**Se acceptă** Proiectul de Hotărâre de Guvern (PHG) și *Legea nr. 209/2026 privind cooperarea polițienească* asigură în prezent transpunerea parțială a acestui act UE, concentrându-se pe cadrul instituțional și pe principiile de cooperare. Specificațiile tehnice detaliate din Anexa la Decizia 2008/616/JAI (privind profilurile ADN, datele dactiloscopice și

			vehiculele) urmează fi transpuse prin ordin interinstituțional între autoritățile desemnate ca Puncte Naționale de Contact (PNC) și Punctul Unic de Contact (PUC). Această abordare asigură adaptarea tehnică necesară la standardele Prüm II, implementarea fiind eșalonată și condiționată de obținerea accesului la infrastructura Uniunii Europene (Router UE, EPRIS, EUCARIS), conform clauzei de intrare în vigoare de la pct. 4 din clauza de adoptare a proiectului.
	13	Prevederile din Anexa nr. 1 (pct. 5.2–5.6, pct. 5.8, pct. 5.10, pct. 5.14, pct. 9.1, pct. 9.5, pct. 10.1, pct. 10.3–10.7, pct. 10.10, pct. 11.1, pct. 11.3–11.4, pct. 12.1–12.4, pct. 14–15, pct. 26.8, pct. 29.3, pct. 35, pct. 36.1, pct. 38, pct. 41–42, pct. 43–48, pct. 49–51, pct. 52–63, pct. 64–73, pct. 74–75, pct. 76–82, pct. 84, pct. 86–87, pct. 89, pct. 92, pct. 94.1, pct. 101.3, pct. 103–104, pct. 109.1 și pct. 111–119.) și Anexa nr. 2 (pct. 4.6, pct. 5, pct. 9–10, pct. 11.1–11.4, pct. 12.1–12.2, pct. 13–17.3, pct. 19.1–19.3, pct. 21, pct. 32, pct. 36–37, pct. 38.1, pct. 39, pct. 41.1, pct. 41.4, pct. 43–48, pct. 49–54, pct. 56, pct. 58–59, pct. 62–66, pct. 68–69, pct. 71–72, pct. 74–78, pct. 79.1–79.3, pct. 81.1, pct. 81.3 și pct. 82–84.) din proiectul hotărârii Guvernului care vizează conectarea și utilizarea Router-ului UE, EPRIS, EUCARIS, ESP, CIR, CRRS, SIS/SIRENE, SIENA, S-TESTA, cooperarea operațională cu eu-LISA, CERT-UE, Europol, Comisia Europeană și Secretariatul General al Consiliului UE, precum și raportarea statistică către organismele Uniunii Europene, nu pot produce efecte juridice și tehnice depline de la data adoptării hotărârii. Aceste prevederi urmează a fi aplicate de la data aderării Republicii Moldova la Uniunea Europeană sau de la data acordării accesului tehnic și juridic la mecanismele respective, după caz. În lipsa unei asemenea clauze, proiectul creează aparența unei aplicabilități imediate a unor mecanisme UE la care Republica Moldova, în calitate de stat candidat, nu are acces deplin. Prin urmare, proiectul urmează a fi completat cu o clauză expresă de aplicare condiționată, iar în tabelele de concordanță prevederile respective urmează a fi calificate, după caz, ca	**Se acceptă** Proiect ajustat prin: - modificarea pct. 4 din clauza de adoptare a PHG; - includerea noului punct 6. în Anexa nr. 1 a proiectului hotărârii de Guvern; - includerea noului punct 43. în Anexa nr. 2 a proiectului hotărârii de Guvern; - includerea noului punct 50. în Anexa nr. 2 a proiectului hotărârii de Guvern; - includerea noului punct 58. în Anexa nr. 2 a proiectului hotărârii de Guvern; - includerea noului punct 67. în Anexa nr. 2 a proiectului hotărârii de Guvern; - includerea noului punct 82. în Anexa nr. 2 a proiectului hotărârii de Guvern. De asemenea a fost completată și Nota de fundamentare urmare obiecției.

		prevederi UE neaplicabile până la aderare sau aplicabile numai după obținerea accesului la infrastructurile Uniunii Europene.	
	14	Pct. 26.6 din Anexa I a proiectului național, face referire la „dreptul intern al statului membru al autorității judiciare competente”. Pentru Republica Moldova, până la aderare, trebuie utilizată o formulă adaptată: „dreptul intern al Republicii Moldova” sau „dreptul intern al statului solicitat/solicitant, după caz”. Menținerea formulei „stat membru” poate genera confuzie privind aplicarea normei în raport cu statutul actual al Republicii Moldova.	**Se acceptă** Proiect ajustat prin: - modificarea subpct. 27.6. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	15	Proiectul operează cu trimitere la Legea privind cooperarea polițienească internațională (număr unic 264/MAI/2026), care este încă în curs de promovare Adoptarea hotărârii înainte de intrarea în vigoare a legii ar putea crea o problemă de legalitate, deoarece atribuțiile PUC și PNC sunt fundamentate expres în lege. Prin urmare, recomandăm corelarea calendarului de adoptare astfel încât hotărârea să fie aprobată și să intre în vigoare numai după publicarea și intrarea în vigoare a Legii privind cooperarea polițienească internațională.	**Se acceptă** La promovarea și adoptarea proiectului vor fi respectate prevederile Legii nr. 100/2017 cu privire la actele normative, inclusiv cerințele privind corelarea actelor normative și intrarea lor în vigoare. În acest sens, hotărârea va fi aprobată și va intra în vigoare în concordanță cu prevederile Legii nr. 209/2026 privind cooperarea polițienească internațională, astfel încât să fie asigurată baza legală necesară pentru exercitarea atribuțiilor PUC și PNC și să fie evitate eventuale probleme de legalitate.
	16	Pct. 4, 40.2, 62, 101.3 din Anexa 1 și pct. 36, 72 a Anexei 2 din proiectul național operează cu trimiteri directe la Directiva (UE) 2023/977, Regulamentul (UE) 2016/794, Regulamentul (UE) 2024/982. Ținând cont că, potrivit normelor de tehnică legislativă națională, nu sunt admisibile trimiterile directe la actele juridice europene, trimiterea fie se va exclude, fie se va substitui cu trimiteri la prevederile actelor normative naționale care au asigurat transpunerea actelor UE sus enunțate.	**Se acceptă** Proiect ajustat prin: - modificarea pct. 4., subpct. 41.2., pct. 64 și subpct. 102.3. din Anexa nr. 1 a proiectului hotărârii de Guvern, precum și pct. 36 și pct. 74. din Anexa nr. 2 a proiectului hotărârii de Guvern.
	17	Clauza de armonizare a proiectului de lege urmează a fi expusă în următoarea redacție: **„Prezenta Hotărâre:** - **transpune parțial Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024 privind căutarea și schimbul automatizat de date în scopul cooperării polițienești, și de**	**Se acceptă** Partea dispozitivă a proiectului hotărârii de Guvern modificată.

		modificare a Deciziilor 2008/615/JAI și 2008/616/JAI ale Consiliului și a Regulamentelor (UE) 2018/1726, (UE) 2019/817 și (UE) 2019/818 ale Parlamentului European și ale Consiliului (Regulamentul Prüm II), publicat în Jurnalul Oficial al Uniunii Europene L 2024/982 din 5 aprilie 2024, CELEX: 32024R0982; **- transpune parțial Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere, publicată în Jurnalul Oficial al Uniunii Europene, L 210 din 6 august 2008, așa cum a fost modificată ultima oară prin Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024, CELEX: 32008D0615;** **- transpune parțial Decizia 2008/616/JAI a Consiliului din 23 iunie 2008 privind punerea în aplicare a Deciziei 2008/615/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere, publicată în Jurnalul Oficial al Uniunii Europene, L 210 din 6 august 2008, așa cum a fost modificată ultima oară prin Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024, CELEX: 32008D0616;** **- transpune parțial Decizia 2004/919/CE a Consiliului din 22 decembrie 2004 privind combaterea criminalității referitoare la vehicule și având implicații transfrontaliere, publicată în Jurnalul Oficial al Uniunii Europene, L 389/28 din 30 decembrie 2004, CELEX: 320004D0919;** **- transpune parțial Directiva 2023/977 a Parlamentului European și al Consiliului din 10 mai 2023 privind schimbul de informații dintre autoritățile de aplicare a legii ale statelor membre și de abrogare a Deciziei-cadru 2006/960/JAI a Consiliului, publicată în Jurnalul Oficial al Uniunii Europene, L 134/1 din 22 mai 2023, CELEX: 32023L0977;** **- transpune parțial Poziția comună 2005/69/JAI a Consiliului din 24 ianuarie 2005 privind schimbul de anumite date cu Interpol, publicată în Jurnalul Oficial al Uniunii Europene, L 27/61 din 29 ianuarie 2005, CELEX: 32005E0069.”**	
Centrul Național de Expertize Judiciare	**18**	Utilizarea terminologiei de „expert calificat” (pct. 8.3 și pct. 45 din proiect) pentru persoanele care efectuează revizuirea manuală a	**Se acceptă** Proiect ajustat prin:

(nr. 134/08 din 26.05.2026)		concordanțelor (hit-urilor) aduce atingere principiilor de activitate în domeniul expertizei judiciare. În conformitate cu legislația națională, expertiza judiciară este o activitate procesuală strict reglementată. Utilizarea termenului „expert" într-un context administrativ sau de schimb de date între baze de date poate crea confuzie între o verificare tehnică de rutină și o expertiză judiciară ordonată de un organ de urmărire penală sau de instanță. Conform HG nr. 821/2023, personalul implicat în gestionarea bazelor de date genetice are interdicția de a efectua expertize judiciare în specialitatea „expertiză genetică" pe perioada exercitării funcției. Astfel, atribuirea calității de „expert" unei persoane care efectuează validarea hit-urilor biometrice intră în contradicție directă cu normele de integritate și imparțialitate specifice domeniului. Mai mult, Regulamentul (UE) 2024/982 (Prüm II) consacră termenul de „membru calificat" tocmai pentru a asigura o separare riguroasă între atribuțiile operative de verificare a datelor și activitatea de expertiză judiciară. Această distincție este imperativă deoarece rolurile sunt, prin natura lor, incompatibile; orice confuzie între ele ar genera un risc iminent de viciere a probelor și de compromitere a integrității bazelor de date. Din considerentele expuse, în vederea asigurării respectării cadrului juridic ce guvernează profesia de expert judiciar, se impun următoarele modificări în Anexa nr. 2 a proiectului: Subpunctul 8.3 din Capitolul II și Punctul 45 din Capitolul VII: Înlocuirea sintagmei „expert calificat" cu termenul „membru calificat" sau „specialist". În acest context, este de menționat că modificare propusă va asigura că validarea hit-urilor este percepută ca o etapă tehnică de verificare a calității datelor și nu ca o concluzie de expertiză judiciară cu valoare probatorie preconstituită.	- modificarea pct. 8.3., și pct. 44. din Anexa nr. 2 a proiectului hotărârii de Guvern.
Centrul Național pentru Protecția datelor cu Caracter Personal (nr. 04-01/2081 din 10.06.2026)	**19**	Cu referire la art. 110 din Anexa nr. 1 și art. 42 din Anexa nr. 2 ale proiectului, se recomandă completarea prevederilor privind formele de răspundere prin includerea răspunderii administrative. Această necesitate rezultă din faptul că Legea nr. 195/2024 privind protecția datelor cu caracter personal (care va intra în vigoare la 23 august 2026) instituie răspunderea administrativă pentru încălcarea dispozițiilor sale, inclusiv sub forma sancțiunilor pecuniare. În acest sens, norma propusă urmează să reflecte în mod complet și fidel regimul general al răspunderii aplicabil în domeniul protecției datelor cu caracter personal.	**Se acceptă** A se vedea argumentarea la obiecția cu nr. 82.

Consiliul Superior al Magistraturii (nr. 1612m/c din 10.06.2026)	**20**	În partea dispozitivă a proiectului hotărârii sunt desemnate Punctele Naționale de Contact, dar Punctul Unic de Contact pare să fie identificat mai clar abia în anexă, unde se spune că funcțiile PUC sunt exercitate de Direcția cooperare polițienească internațională a IGP. Pentru claritate juridică, desemnarea PUC ar trebui inclusă expres în textul hotărârii, nu doar în regulamentul anexat.	**Nu se acceptă** Punctul Unic de Contact (PUC) este instituit și desemnat prin Legea nr. 209/2026 privind cooperarea polițienească internațională, care stabilește statutul, atribuțiile și cadrul de funcționare al acestuia. Proiectul hotărârii Guvernului are caracter subsecvent și reglementează aspectele organizatorice și procedurale aferente exercitării funcțiilor PUC, motiv pentru care nu este necesară o desemnare distinctă a acestuia în partea dispozitivă a hotărârii.
	21	Proiectul utilizează frecvent sintagme preluate din dreptul UE: „*stat membru solicitant*”, „*stat membru solicitat*”, „*state membre ale Uniunii Europene*”, dar Republica Moldova nu are încă această calitate. Mai multe acte specifică calitate de stat candidat la aderarea la Uniunea Europeană (pct. 11 al Concluziilor Consiliului European din 23-24 iunie 2022, document EUCO 24/22). Prin urmare propunem nuanțarea după caz a acestui aspect pentru reducerea confuziei privind drepturile și obligațiile Republicii Moldova în procesul descris în proiect.	**Se acceptă** Textul proiectului a fost revizuit integral pentru a elimina ambiguitățile privind drepturile și obligațiile Republicii Moldova în raport cu statutul său actual de stat candidat.
	22	Cu referire la pct. 4 din proiectul hotărârii de Guvern, prin care se stabilește că „*prezenta hotărâre intră în vigoare la data intrării în vigoare a Legii privind cooperarea polițienească internațională*”, se reține că o asemenea formulare este admisibilă doar în măsura în care actul de bază, *i.e. Legea privind cooperarea polițienească internațională*, este deja adoptat și publicat, iar/sau data intrării în vigoare este cert determinată sau determinabilă. Potrivit art. 56 din Legea 100/2017 *privind actele normative*, actele normative intră în vigoare la data indicată în text, care nu poate fi anterioară publicării, iar stabilirea unei date de intrare în vigoare poate fi realizată doar în condițiile expres prevăzute de lege, inclusiv pentru asigurarea corelării sistemului normativ. În speță, întrucât Legea privind cooperarea polițienească internațională se află încă în curs de promovare, se recomandă revizuirea pct. 4 din proiect, în sensul stabilirii unei date certe de intrare în vigoare sau, după caz,	**Se acceptă** A se vedea argumentarea la obiecția cu nr. 15.

		corelării acesteia cu momentul publicării și intrării în vigoare efective a legii menționate, cu respectarea exigențelor prevăzute de art. 56 din Legea nr. 100/2017.	
	23	La ***pct. 3, 5-7, 93-94 din Anexa 1 „Regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații”***, precum și ***pct. 7, 34 din Anexa 2 „ Regulamentul de organizare și funcționare a Punctelor Naționale de Contact în scopul schimbului de date și informații”*** se face trimitere la *Legea privind cooperarea polițienească internațională*, care nu este încă adoptată. Trimiterile la articolele legii trebuie verificate după forma finală a acesteia. Aceasta rezultă și din art. 3 alin (4) din Legea nr. 100, potrivit căruia proiectul întocmit în temeiul unui act superior nu poate depăși limitele competenței instituite prin actul superior. Mai mult decât atât, în proiectul cu numărul unic 264/MAI, Legea figurează sub altă denumire – Legea privind căutarea și schimbul de date în scopul cooperării polițienești transfrontaliere.	**Se acceptă** Trimiterile la prevederile Legii nr. 209/2026 privind cooperarea polițienească internațională vor fi reverificate și ajustate corespunzător după adoptarea și publicarea legii, inclusiv sub aspectul numerotării articolelor, denumirii actului normativ și al corelării cu forma finală a acesteia, în conformitate cu cerințele Legii nr. 100/2017 cu privire la actele normative.
	24	Cu referire la prevederile din ***Anexa 1 „Regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații”***, și ***Anexa 2 „ Regulamentul de organizare și funcționare a Punctelor Naționale de Contact în scopul schimbului de date și informații”,*** referitoare la funcționarea mecanismelor și sistemelor de cooperare la nivelul Uniunii Europene (Router UE, EPRIS, EUCARIS, ESP, CIR, CRRS, SIS/SIRENE, SIENA, S-TESTA), precum și cele privind cooperarea operațională cu eu-LISA, CERT-UE, Europol, Comisia Europeană și Secretariatul General al Consiliului Uniunii Europene, inclusiv raportarea statistică către aceste entități, propunem reformularea într-o clauză de aplicare etapizată – „*Prevederile referitoare la utilizarea sistemelor, infrastructurilor, canalelor de comunicații și mecanismelor de cooperare ale Uniunii Europene se aplică de la data asigurării accesului juridic și tehnic al Republicii Moldova la acestea, în condițiile tratatelor internaționale, acordurilor operaționale, actelor normative UE aplicabile și cadrului normativ național.*”. Această formulă evită atât falsa aplicabilitate imediată. Cât și blocarea nejustificată până la aderarea formală.	**Se acceptă** Proiectul a fost ajustat prin modificarea pct. 4 din clauza de adoptare a PHG, care asigură realismul juridic și tehnic al reglementării în raport cu statutul actual al Republicii Moldova. Această modificare elimină riscul unei false aplicabilități imediate a mecanismelor la care statul nu are încă acces, permițând totodată pregătirea instituțională necesară integrării europene. Modificare survenită în baza obiecției cu nr. 13.
	25	La **pct. 10.10 din** ***Anexa 1 „Regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și***	**Se acceptă** Proiectul a fost ajustat prin:

		informații”, care se referă la accesul personalului desemnat pentru cooperarea cu Europol la „*toate bazele de date naționale relevante*”. Considerăm formularea prea extensivă și propunem o formulare mai restrictivă: „*la bazele de date stabilite expres prin lege sau prin acte normative aplicabile, în limitele competențelor, scopului determinat, necesității și proporționalității*”.	- modificarea subpct. 11.10. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	26	La **pct. 24 din *Anexa 1 „Regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații”***, se prevede posibilitatea prelungirii termenelor de soluționare a cererilor în cazuri excepționale, atunci când solicitarea implică un volum mare de date și necesită consultarea mai multor autorități sau efectuarea unor verificări complexe. Această soluție necesită revizuire, întrucât art. 5 alin. (2) din Directiva (UE) 2023/977 stabilește termene maxime obligatorii de răspuns, iar derogările de la acestea trebuie interpretate în mod restrictiv. Potrivit dispozițiilor Directiva (UE) 2023/977 (art. 5 alin.2), termenele maxime sunt de 8 ore pentru informațiile direct accesibile în cazuri urgente, 3 zile pentru informațiile indirect accesibile în cazuri urgente și 7 zile pentru celelalte solicitări. Prelungirea acestor termene este admisibilă exclusiv în ipotezele expres și limitativ prevăzute, respectiv atunci când este necesară obținerea unei autorizații judiciare, cu obligația informării imediate a autorității solicitante și a transmiterii etapizate a datelor disponibile. Derogarea de la termene se admite doar în condițiile expres prevăzute, în special când este necesară autorizația judiciară; celelalte situații trebuie reglementate ca proceduri de notificare/refuz/furnizare parțială, nu ca prelungire generală. În consecință, se recomandă reformularea pct. 24 din Anexa nr. 1 prin eliminarea temeiurilor de prelungire care nu sunt prevăzute de directivă, precum „*volumul mare de date*” sau „*complexitatea verificărilor implicând mai multe autorități*”, și limitarea expresă a derogărilor exclusiv la cazurile de autorizare judiciară și imposibilitate obiectivă de furnizare a informațiilor, cu menținerea obligației de comunicare imediată și de transmitere parțială a datelor disponibile.	**Se acceptă** Proiectul a fost ajustat prin: - modificarea pct. 25 din Anexa nr. 1 a proiectului hotărârii de Guvern. Modificare survenită în baza obiecției cu nr. 9.
	27	Potrivit **pct. 26.3 din *Anexa 1 „Regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații”*** – examinarea cererilor de autorizare judiciară se realizează prin mecanisme de permanență (24/7). Această prevedere vizează instanțele	**Se acceptă** Proiectul a fost ajustat prin: - modificarea pct. 27 din Anexa nr. 1 a proiectului hotărârii de Guvern.

		judecătorești și/sau judecătorii de instrucție, și trebuie corelat cu Codul de procedură penală. Cu legislația privind organizarea judecătorească și cu actele CSM privind organizarea serviciului, în limitele competenței legale. Propunem reglementarea exactă a aspectelor ce țin de tipurile de informații care necesită autorizație judiciară, cine este autoritatea competentă, care este procedura, care sunt termenele și, eventual, modificarea Codului de procedură penală sau a altor acte.	
	28	**În partea ce ține de protecția datelor și accesul la baze de date**, proiectul prevede schimb de date biometrice, date dactiloscopice, imagini faciale, documente de călătorie, date privind persoane urmărite, dispărute sau implicate în activități infracționale. În acest sens propunem delimitarea expresă a categoriilor de date, a temeiului de acces, a autorităților care pot solicita/furniza date, a perioadelor de stocare și a garanțiilor împotriva accesului disproporționat.	**Se acceptă** Proiectul de hotărâre a fost structurat astfel încât să asigure o delimitare riguroasă a tuturor elementelor solicitate pentru protecția datelor cu caracter personal și prevenirea accesului disproporționat, prin: - delimitarea categoriilor și autorităților (fiecare domeniu de date se regăsește la anumit PNC); - temeiul și condițiile de acces; - perioade de stocare; - garanții procedurale; - control (rolul CNPDCP).
	29	**Proiectul prevede că toate operațiunile de acces și de schimb de date sunt înregistrate „*Sistemului electronic unic de gestionare a cazurilor*”**. Propunem indicarea în act a temeiului juridic al sistemului, administratorul, operatorul de date, modul de acces, regimul de audit și relația cu SIENA. Astfel, norma riscă să fie prea generală pentru un sistem care va prelucra date sensibile.	**Se acceptă** Proiectul a fost ajustat prin: - modificarea pct. 37 și pct. 38. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	30	**În partea ce ține de nota de fundamentare,** în proiect apare o formulare care pare eronată: se vorbește despre „*proiectul hotărârii Guvernului pentru aprobarea proiectului de lege pentru modificarea Legii nr. 288/ privind funcționarul public cu statut special [...]*”, deși proiectul examinat este despre PUC și PNC. La secțiunea 8 a notei se afirmă că proiectul nu impune modificarea sau abrogarea unor acte normative, dar ulterior, la secțiunea 9 – se menționează că vor fi modificate fișele de post și regulamentele de activitatea ale subdiviziunilor/autorităților implicate. Considerăm oportună semnalizarea acestei observații.	**Se acceptă** Nota de fundamentare a fost completată ca urmare a obiecției.

	31	**La secțiunea 4.2. Impactul financiar și argumentarea costurilor estimative**. Nota de fundamentare spune că proiectul nu necesită cheltuieli suplimentare, deși proiectul presupune funcționare 24/7, interoperabilitate, instruirea personalului, conectivitate securizată, administrare de log-uri, raportare statistică și eventual implicarea instanțelor în mecanisme de permanență. Această contradicție este esențială, cel puțin în partea care vizează instanțele și CSM.	**Se acceptă** Nota de fundamentare a fost completată ca urmare a obiecției.
Agenția de Guvernare Electronică (nr. 3007-180 din 12.06.2026)	**32**	La pct. 10. din proiect, sintagma „PUC acționează ca interfață unică și centralizată între sistemele informaționale naționale și infrastructura centrală a Uniunii Europene" urmează a fi revizuită, deoarece atribuie unei structuri administrative o calificare de natură tehnică incompatibilă cu regimul juridic al sistemelor informaționale de stat. Conform logicii proiectului, PUC este o structură administrativă și operațională creată ca să coordoneze și să gestioneze schimbul de date și informații prin intermediu infrastructurii tehnice prevăzute de Regulamentul (UE) 2024/982 și nu pate fi asimilată unei interfețe tehnice între sistemele informaționale. Astfel, terminologia urmează a fi revăzută și aliniată la Regulamentul (UE) 2024/982, care atribuie funcția de interconectare a Router-ului gestionat de eu-LISA, iar funcția de coordonare operațională națională, este atribuită punctului național desemnat de statul membru.	**Se acceptă** Proiectul a fost ajustat prin: - modificarea pct. 11. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	33	Pct.10.5 și 10.6 atribuie PUC realizarea schimbului de date prin EPRIS, însă datele circulă prin Router și nu prin EPRIS. Conform art. 42 din Regulamentul (UE) 2024/982, EPRIS este un sistem cu infrastructură descentralizată, adică fiecare stat membru menține propriile registre naționale, iar EPRIS este instrumentul de căutare care interoghează simultan aceste registre naționale. Statul membru nu se conectează la EPRIS ca la o bază de date externă în care introduce date, ci EPRIS vine și interoghează registrul național existent al statului.	**Se acceptă** Proiectul a fost ajustat prin: - modificarea subpct. 11.4. și subpct. 11.5. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	34	Pct. 10.6 atribuie PUC realizarea schimbului de date prin EUCARIS pentru informațiile privind mijloacele de transport. Atragem atenția că Agenția Servicii Publice, în calitate de posesor al Registrului de stat al vehiculelor este desemnată separat, în pct. 1.4 al proiectului hotărârii, ca punct național de contact pentru datele privind mijlocele de transport. Astfel, constatăm o suprapunere între atribuțiile PUC și atribuțiile ASP ca punct național de contact tehnic.	**Se acceptă** Proiectul a fost ajustat prin: - modificarea pct. 11.6. din Anexa nr. 1 a proiectului hotărârii de Guvern.

		Suplimentar, menționăm că EUCARIS acționează similar ca EPRIS. Acesta interconectează sistemele informaționale naționale. Fiecare stat participant comunică direct cu celelalte prin EUCARIS, pe baza datelor din propriul registru național al vehiculelor.	
	35	Aceeași problemă o constatăm și la pct. 10.8. Reiterăm că PUC nu este o interfață și nu acționează prin interfață, așa cum menționează pct. 10.8. SLTD este o bază de date a Interpol, accesul la care se realizează prin canalele securizate ale Interpol. PUC nu se conectează direct la SLTD, ci Interpol este cel care asigură interfața tehnică. O altă problemă legată de SLTD este faptul că aceasta nu face parte din cadrul Prüm II și nu este reglementată de Regulamentul (UE) 2024/982. SLTD este un sistem al Interpol, separat de infrastructura UE descrisă în proiect (Router, EPRIS, EUCARIS). Includerea atribuțiilor privind SLTD în același punct care reglementează funcțiile PUC în cadrul Prüm II creează o fuziune a două regimuri juridice distincte, cel al cooperării polițienești UE și cel al cooperării prin Interpol, fără a delimita temeiul legal aplicabil fiecăruia, procedurile specifice, garanțiile de protecție a datelor aferente și autoritățile responsabile. Pct. 10.8 urmează a fi reformulat cu delimitarea clară a temeiului juridic aplicabil schimbului de date prin baza de date SLTD a Interpol față de mecanismele prevăzute de Regulamentul (UE) 2024/982.	**Se acceptă** Proiectul a fost ajustat prin: - modificarea pct. 11.8. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	36	Suplimentar, AGE constată că proiectul avizat invocă în clauza de adoptare Legea privind cooperarea polițienească internațională, ca temei legal, cu coordonate de publicare în Monitorul Oficial cu placeholder-uri (nr. YYY YYY, art. ZZZ), ceea ce confirmă că legea și respectiv un temei legal, nu există deocamdată. Totodată, din documentele disponibile public, proiectul de lege circulă sub denumirea Legea privind căutarea și schimbul de date în scopul cooperării polițienești transfrontaliere (NU 264/MAI/2026), denumire complet diferită față cea invocată în proiect și nota de fundamentare. Această neconcordanță creează o problemă prin faptul că nu se poate stabili cu certitudine dacă proiectul vine întru implementarea viitoarei legi cu număr unic 264/MAI/2026 sau a unui alt proiect de lege cu obiect diferit, ori dacă cele două proiecte sunt variante ale aceluiași act normativ aflat în elaborare. Astfel, comunicăm, că coordonarea unui proiect de hotărâre a Guvernului, subsecvent unui cadru legal incert la această etapă, face imposibilă verificarea coerenței sistemice dintre actele	**Se acceptă** A se vedea argumentarea la obiecția cu nr. 15. Totodată reiterăm faptul că *legea nr. 209/2026 privind cooperarea polițienească internațională* a fost avizat de către AGE prin scrisoarea cu nr. 3007-086 din 09.04.2026.

		normative. În aceste condiții, AGE recomandă coordonarea repetată a proiectului, după adoptarea Legii cadru. Concomitent, urmare a unei analize preliminare a proiectului legii cu număr unic 264/MAI/2026, constatăm că acesta reglementează instituirea și funcționarea unui sistem informațional (Sistemul electronic unic de gestionare a cazurilor), precum, și modalități de interconectare a registrelor naționale cu infrastructura tehnică internațională. Respectiv, la fel cum este indicat în precizarea de la pct.2.1 din nota de fundamentare, se impune coordonarea cu AGE a proiectului legii privind cooperarea polițienească internațională/privind căutarea și schimbul de date în scopul cooperării polițienești transfrontaliere, pentru a asigura conformitatea dispozițiilor privind sistemele informaționale de stat cu cadrul normativ național în domeniu și coerența cu platformele și serviciile guvernamentale partajate.	
Institutul Național al Justiției (nr. 329-INJ din 12.06.2026)	**37**	Potrivit punctului 9 din nota de fundamentare, implementarea proiectului necesită instruirea personalului implicat în schimbul de informații. Totodată, mecanismele instituite — în special procedura autorizării judiciare reglementată în Secțiunea a 6-a din Anexa nr. 1 — angrenează în mod direct judecători și procurori, categorii care beneficiază de formarea inițială și continuă asigurată de Institutul Național al Justiției. În acest context, propunem completarea măsurilor cu indicarea unor mecanisme clare legate de instruirea personalului.	**Se acceptă** Nota de fundamentare a fost completată pentru a detalia mecanismele de instruire a personalului implicat. S-a stabilit o distincție clară între instruirea tehnică a personalului PUC/PNC (coordonată prin Consiliul de Coordonare eu-LISA conform Ordinului Comun din 30.03.2026) și formarea juridică a magistraților. În acest sens, se va institui un mecanism de colaborare cu Institutul Național al Justiției pentru actualizarea curriculei de formare continuă a procurorilor și judecătorilor de instrucție, vizând noile proceduri de autorizare judiciară reglementate în Secțiunea a 6-a din Anexa nr. 1. Această măsură va asigura că sistemul judiciar este pregătit să răspundă termenelor stricte de furnizare a informațiilor (8h, 3z, 7z) impuse de standardele europene.
	38	Cu referire la mecanismul de permanență (24/7) pentru examinarea cererilor de autorizare judiciară, prevăzut în aceeași secțiune, recomandăm clarificarea autorității competente să dispună autorizarea (judecătorul de	**Se acceptă** Proiect ajustat prin:

		instrucție sau, după caz, procurorul) și corelarea procedurii cu prevederile Codului de procedură penală. Întrucât instituirea unui regim de permanență cu impact asupra organizării activității instanțelor și a procuraturii presupune coordonarea cu Consiliul Superior al Magistraturii și Procuratura Generală, sugerăm consultarea acestor autorități cu privire la soluția operațională și la resursele necesare.	- modificarea pct. 27. din Anexa nr. 1 a proiectului hotărârii de Guvern. Modificare survenită în baza obiecției cu nr. 27.
	39	Proiectul se întemeiază pe Legea privind cooperarea polițienească internațională (număr unic 264/MAI), aflată încă în proces de adoptare, intrarea sa în vigoare fiind corelată cu intrarea în vigoare a acestei legi. Atragem atenția asupra necesității corelării depline a trimiterilor interne la articolele legii (în special art. 4, art. 40 și art. 42), astfel încât numerotarea și conținutul acestora să corespundă întocmai textului final al legii adoptate.	**Se acceptă** A se vedea argumentarea la obiecția cu nr. 15.
	40	În ceea ce privește prelucrarea datelor cu caracter personal, proiectul face, pe alocuri, trimitere generică la „legislația națională privind protecția datelor”. Pentru claritate și previzibilitate, recomandăm indicarea expresă a Legii nr. 133/2011 privind protecția datelor cu caracter personal și, după caz, a cadrului normativ special aplicabil prelucrării datelor în scopul prevenirii, depistării și investigării infracțiunilor, inclusiv corelarea cu atribuțiile Centrului Național pentru Protecția Datelor cu Caracter Personal.	**Se acceptă** Proiectul a fost ajustat prin: - modificarea pct. 35., pct. 91. și pct. 104. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	41	Dispozițiile privind răspunderea juridică fac trimitere generică la Codul contravențional și la Codul penal. În măsura posibilului, recomandăm indicarea normelor concrete de referință, în scopul sporirii rigorii și a aplicabilității reglementării. La fel, recomandăm excluderea de la pct. 108 din Regulament a sintagmei „*...a personalului vinovat*”. Considerăm că tragerea la răspundere juridică presupune de la sine constatarea unei forme a vinovăției. Respectiv, este o chestiune care se prezumă.	**Se acceptă parțial** Proiectul a fost ajustat prin: - modificarea pct. 109. din Anexa nr. 1 a proiectului hotărârii de Guvern, precum și pct. 40. din Anexa nr. 2 a proiectului hotărârii de Guvern.
	42	Semnalăm câteva erori materiale care necesită corectare: în Anexa nr. 1, titlul „STRUCTURA ȘI MODUL DE ORGANIZARE ȘI FUNCȚIONARE AL PUCTULUI UNIC DE CONTACT” (corect: „PUNCTULUI”); sintagma „documente de că călătorie” (corect: „documente de călătorie”); codul „CELEX: 320004D0919” din clauza de transpunere (corect: „32004D0919”). De asemenea, în nota de fundamentare se impun corectarea sintagmei „schimbului schimbului de date” din titlu și a abrevierii „profile AND” (corect: „ADN”).	**Se acceptă** Textele proiectului și a Notei de Fundamentare au fost modificate.
	43	Recomandăm verificarea integrală a sistemului de trimiteri interne (referințele de tipul „pct. ...”), astfel încât, după stabilirea numerotării finale	**Se acceptă**

		a punctelor, fiecare trimitere să corespundă exact dispoziției vizate. Totodată, sugerăm uniformizarea terminologiei și a abrevierilor utilizate pe parcursul textului (de exemplu, folosirea consecventă a formei „CTCEJ”).	A se vedea argumentarea la obiecția cu nr. 23. Ce ține de uniformizarea terminologiei și a abrevierilor CTCEJ, proiectul a fost ajustat.
Ministerul Afacerilor Externe (nr. DI/3/041.1-6126 din 27.05.2026)	**44**	La pct. 6.1 din Anexa nr. 1 la proiectul Hotărârii Guvernului, sintagma „tratatelor internaționale” se va completa cu expresia „la care Republica Moldova este parte”.	**Se acceptă** Subct. 7.1. din Anexa nr. 1 a proiectului hotărârii de Guvern a fost modificat a fost modificat.
Ministerul Finanțelor (nr. 07/4-03/197/909 din 12.06.2026)	**45**	La Capitolul I, pct. 5.11., Anexa nr. 1 din Regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații, cuvintele „vamă” și „fisc” se vor substitui cu sintagmele „Serviciul Vamal” și, respectiv, „Serviciul Fiscal de Stat”.	**Se acceptă** Subct . 5.11. din Anexa nr. 1 a proiectului hotărârii de Guvern a fost modificat.
	46	La Capitolul IV, Secțiunea 1., Anexa nr. 1 din Regulament, după punctul 63 se propune de completat cu un punct nou cu următorul cuprins: „*Pentru asigurarea conformității cu prevederile pct. 63, orice căutare și interogare automatizată realizată prin intermediul Router-ului, al ESP sau CIR, inclusiv cele care vizează date biometrice și imagini faciale, generează în mod obligatoriu o pistă de audit (log-uri) nealterabilă, păstrată pe o perioadă de minimum 5 ani. Pista de audit va stoca în mod automat: numărul cazului individual/dosarului penal, temeiul juridic al verificării, identificatorul de utilizator, data/ora exactă, tipul de date biometrice procesate și rezultatul concordanței transmise.*”. Modificarea propusă este indispensabilă pentru a asigura o protecție reală a datelor cu caracter personal și pentru a transforma obligația de la pct. 63 dintr-o normă declarativă într-una aplicabilă și verificabilă juridic. Având în vedere că punctele 56, 57 și 59 prevăd procesarea automatizată a unor date de o sensibilitate extremă (biometrice și imagini faciale), iar pct. 55 reglementează transmiterea automată a concordanțelor înapoi către Router, riscul de imixtiune ilegală în dreptul la viața privată este major. În lipsa acestei piste de audit detaliate, autoritățile naționale de supraveghere vor fi în imposibilitate tehnică și juridică de a verifica dacă schimburile de date, inclusiv cele cu țări terțe prin Europol (conform pct. 62), s-au efectuat cu respectarea garanțiilor din dreptul intern.	**Se acceptă** Proiectul a fost ajustat prin: - includerea noului punct cu nr. 61 în Anexa nr. 1 a proiectului hotărârii de Guvern.
	47	Totodată, deși, în pct. 4.2. „*Impactul financiar și argumentarea costurilor estimative*” din Nota de fundamentare se menționează că implementarea proiectului de hotărâre nu va avea impact financiar	**Se acceptă** Nota de fundamentare a fost completată ca urmare a obiecției.

		suplimentar asupra bugetului de stat, iar dezvoltarea și sincronizarea sistemelor informaționale urmează a fi asigurate în limitele bugetului de stat aprobat anual, autorul urmează să specifice nemijlocit costul estimativ al dezvoltării și sincronizării sistemelor informaționale, în vederea asigurării transparenței procesului de planificare bugetară și a evaluării impactului financiar real al proiectului.	
Ministerul Justiției (nr. 04/1-6337 din 10.06.2026)	**48**	Totuși, ținem să subliniem că proiectul nu poate fi promovat anterior publicării Legii privind cooperarea polițienească internațională.	**Se acceptă** A se vedea argumentarea la obiecția cu nr. 15.
	49	În clauza de adoptare textul „alin. (2), alin. (6) și alin. (7)” se va substitui cu textul „alin. (2), (6) și (7)”, or, într-o enumerare de referințe, denumirea elementului structural nu se repetă. Adițional, sursa de publicare va include și anul publicării.	**Se acceptă** Clauza de adoptare modificată.
	50	Din liniuța a patra din clauza de armonizare se va exclude cuvântul „transpune” ca fiind excedent.	**Se acceptă** Clauza de adoptare modificată.
	51	La utilizarea abrevierilor se va ține cont că, potrivit art. 54 alin. (1) lit. i) din Legea nr. 100/2017 cu privire la actele normative, exprimarea prin abrevieri a unor denumiri sau termeni se poate face numai după explicarea acestora în text, la prima folosire.	**Se acceptă** Textul proiectului hotărârii de Guvern ajustat.
	52	La subpct. 1.2 se va reformula statutul Serviciului Tehnologii Informaționale, or, potrivit pct. 2 din Regulamentul privind organizarea și funcționarea Serviciului Tehnologii Informaționale, aprobat prin Hotărârea Guvernului nr. 317/2020, acesta este autoritate administrativă în subordinea Ministerului Afacerilor Interne.	**Se acceptă** Subpct. 1.2. din clauza de adoptare a PHG a fost modificat.
	53	La subpct. 1.3 se va reformula statutul Inspectoratului General de Carabinieri, or, potrivit pct. 2 din Regulamentul cu privire la organizarea și funcționarea Inspectoratului General de Carabinieri, aprobat prin Hotărârea Guvernului nr. 332/2019, Inspectoratul este autoritate administrativă, subordonată Ministerului Afacerilor Interne.	**Se acceptă** Subpct. 1.3. din clauza de adoptare a PHG a fost modificat.
	54	Observațiile la subpct. 1.2 și 1.3 sunt valabile și pentru anexa nr. 2.	**Se acceptă** Textul proiectului a fost modificat.
	55	La subpct. 1.5 se va utiliza noțiunea „infracțiunilor cu caracter terorist”, în acord cu prevederile art. 134^{11} din Codul penal nr. 985/2002. Observația dată este valabilă pentru toate cazurile similare din proiect.	**Se acceptă** Proiect ajustat prin: - modificarea subpct. 1.5. din clauza de adoptare a PHG; - modificarea subpct. 4.5. din Anexa nr. 2 a proiectului hotărârii de Guvern;

			- modificarea textului Secțiunii 1 a Capitolului XI. din Anexa nr. 2 a proiectului hotărârii de Guvern; - modificarea pct. 74. din Anexa nr. 2 a proiectului hotărârii de Guvern.
	56	La pct. 4, norma privind intrarea în vigoare urmează a fi completată prin raportare la art. 56 alin. (1) din proiectul Legii privind cooperarea polițienească internațională (număr unic 264/MAI/2026). Or, deși proiectul prevede intrarea în vigoare a hotărârii la data intrării în vigoare a legii, dispozițiile referitoare la Biroul Național SIRENE și Sistemul de Informații Schengen pot fi aplicate numai de la data aderării Republicii Moldova la mecanismele respective.	**Se acceptă** Norma privind intrarea în vigoare modificată conform pct. 4 din clauza de adoptare a PHG. Modificare survenită în baza obiecțiilor cu nr. 13 și nr. 24.
	57	Prin urmare, se va prevedea expres că normele aferente Biroului Național SIRENE și Sistemului de Informații Schengen se aplică de la data aderării Republicii Moldova la aceste mecanisme. Observația vizează, în special, pct. 9 subpct. 5), pct. 10 subpct. 3) și 7) din anexa nr. 1, precum și pct. 63, 65, 68 și pct. 79 subpct. 3) din anexa nr. 2.	**Se acceptă** Proiect ajustat prin: - modificarea pct. 4 din clauza de adoptare a PHG. Modificare survenită în baza obiecțiilor cu nr. 13 și nr. 24.
	58	Totodată, o abordare similară urmează a fi aplicată prevederilor referitoare la Router, EPRIS, CIR, ESP, CRRS și la alte sisteme sau infrastructuri ale Uniunii Europene, întrucât intrarea în vigoare a legii nu echivalează, prin ea însăși, cu dobândirea dreptului de acces ori cu autorizarea conectării Republicii Moldova la acestea.	**Se acceptă** Proiect ajustat prin: - modificarea pct. 4 din clauza de adoptare a PHG. Modificare survenită în baza obiecțiilor cu nr. 13 și nr. 24.
	59	***La regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații:*** În parafa de aprobare, textul „nr. ___ din_____ 2026” se va substitui cu textul „nr. ___/2026”. Observația dată este valabilă și pentru anexa nr. 2.	**Se acceptă** Parafele anexelor nr. 1 și nr. 2 modificate.
	60	Cu referire la denumirea Regulamentului, aceasta se va expune după următoarea formulă: „Regulamentul privind organizarea și funcționarea Punctului Unic de Contact în scopul schimbului de date și informații”.	**Se acceptă** Proiect ajustat prin: - modificarea subpct. 2.1. și subpct. 2.2. din clauza de adoptare a PHG; - modificarea denumirii anexelor nr. 1 și nr. 2 a proiectului hotărârii de Guvern.
	61	La pct. 1, enumerarea categoriilor de date urmează a fi revizuită și corelată cu prevederile proiectului de lege privind cooperarea polițienească internațională. În particular, datele dactiloscopice sunt menționate atât în categoria datelor biometrice, cât și distinct, ceea ce generează o dublare	**Se acceptă** Punctul 1 din Anexa nr. 1 modificat.

		nejustificată. Totodată, denumirea celorlalte categorii de date se va uniformiza cu terminologia utilizată în lege.	
	62	La pct. 2, cuvintele „rămășițelor umane” se vor substitui cu cuvintele „cadavre sau părți ale acestora”, în vederea corelării cu terminologia utilizată în Codul de procedură penală nr. 122/2003 (valabil și pentru alte cazuri similare). Subsidiar, pentru o mai bună claritate, se recomandă substituirea cuvintelor „persoanelor dispărute” cu cuvintele „persoanelor dispărute fără veste”, în acord cu prevederile art. 165-167 din Codul civil nr. 1107/2002. Observația dată este valabilă pentru toate cazurile similare din proiect.	**Se acceptă** Proiectul a fost ajustat prin: - modificarea subpct. 1.2 din clauza de adoptare a PHG; - modificarea pct. 1., pct. 2, subpct. 11.5., subpct. 11.9., subpct. 11.11. și pct. 66. din Anexa nr. 1 a proiectului hotărârii de Guvern; - modificarea subpct. 4.2. din Anexa nr. 2 a proiectului hotărârii de Guvern.
	63	La pct. 4, se remarcă faptul că actele juridice ale Uniunii Europene nu sunt direct aplicabile în ordinea juridică națională până la aderarea Republicii Moldova, dacă aplicabilitatea acestora nu rezultă dintr-un temei juridic internațional distinct. Prin urmare, trimiterile la legislația UE se vor exclude sau se vor substitui cu referințe la actele normative naționale prin care au fost transpuse prevederile europene corespunzătoare. Observația dată este valabilă pentru toate cazurile similare din proiect.	**Se acceptă** A se vedea argumentarea la obiecția cu nr. 16.
	64	Alineatul introductiv de la pct. 5 se va reformula după cum urmează: „În sensul prezentului Regulament se utilizează noțiunile definite în Legea privind cooperarea polițienească internațională, precum și următoarele noțiuni:”.	**Se acceptă** Pct. 5 din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.
	65	La subpct. 5.12, se remarcă faptul că introducerea denumirii „Single Point of Contact” și a abrevierii „SPOC” este redundantă și poate genera confuzii, întrucât acestea desemnează aceeași structură ca Punctul Unic de Contact, definit și desemnat prin art. 3 alin. (2), pct. 24 din proiectul legii privind cooperarea polițienească internațională. Prin urmare, se va utiliza în mod unitar denumirea „Punctul Unic de Contact” și abrevierea „PUC”, iar denumirea în limba engleză, după caz, va fi indicată doar cu caracter informativ.	**Se acceptă** Proiectul a fost modificat, cu excepția trimiteri de la pct. 4 din Anexa nr. 1 a proiectului hotărârii de Guvern „(*Single Point of Contact*)”, care este necesar de a fi păstrat, întru asigurarea transpunerii prevederilor Directivei (UE) 2023/977.
	66	La subpct. 6.2, cuvintele „protecția datelor personale” se vor substitui cu cuvintele „protecția datelor cu caracter personal”.	**Se acceptă** Subpct. 7.2. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.
	67	La subpct. 6.4, formula potrivit căreia „orice rezultat este verificat manual de personal calificat” urmează a fi revizuită. Proiectul de lege privind cooperarea polițienească internațională impune verificarea manuală	**Se acceptă** Proiectul a fost ajustat prin:

		pentru confirmarea concordanțelor biometrice, în cazurile expres prevăzute la art. 11, 14 și 19, nu pentru orice rezultat generat de toate sistemele informaționale. Norma urmează să delimiteze rezultatele care sunt supuse obligatoriu verificării manuale.	- modificarea subpct. 7.4.și pct. 78. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	68	La subpct. 9.1, denumirea „Secția Europol” se va corela cu art. 6 alin. (4) din proiectul de lege privind cooperarea polițienească internațională, care utilizează denumirea „Punctul Național de Contact Europol”.	**Se acceptă** Proiectul a fost ajustat prin: - modificarea subpct. 10.1., și subpct. 11.3. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	69	La subpct. 10.1, norma urmează a fi corelată cu art. 53 alin. (7) din proiectul legii privind cooperarea polițienească internațională. Potrivit normei legale menționate, Punctul Unic de Contact notifică Comisia Europeană, eu-LISA și Europol cu privire la identitatea și datele de contact ale punctelor naționale de contact, în timp ce proiectul prevede notificarea Secretariatului General al Consiliului Uniunii Europene și a Comisiei Europene, cu omiterea eu-LISA și a Europol.	**Se acceptă** Subpct. 11.1. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.
	70	La subpct. 18.2, textul „infracțiunii vizate (pregătite sau comise)” este ambiguu și impropriu limbajului juridic. În vederea asigurării clarității normei, se recomandă reformularea după cum urmează: „cu indicarea infracțiunii a cărei pregătire sau săvârșire face obiectul investigației”.	**Se acceptă** Subpct. 19.2. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.
	71	La pct. 24, posibilitatea prelungirii termenelor de soluționare a cererilor urmează a fi revizuită în vederea stabilirii duratei maxime a prelungirii.	**Se acceptă** Proiect ajustat prin: - modificarea și completarea pct. 25. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	72	La subpct. 26.6, cuvintele „dreptul intern al statului membru” urmează a fi adaptate la statutul actual al Republicii Moldova. Or, utilizarea noțiunii „stat membru” poate genera incertitudini privind legea aplicabilă. Prin urmare, se recomandă utilizarea, după caz, cuvintelor „dreptul intern al Republicii Moldova” sau „dreptul intern al statului solicitant ori solicitat”.	**Se acceptă** A se vedea argumentarea la obiecția cu nr. 14.
	73	La subpct. 27.1, se vor exclude cuvintele „din prezentul Regulament”, or, potrivit art. 55 alin. (4) din Legea nr. 100/2017, în cazul în care se face trimitere la o normă juridică care este stabilită în același act normativ sau element structural, pentru evitarea reproducerii acesteia, se face trimitere la norma juridică relevantă fără a se preciza că aceasta face parte din același act normativ sau element structural, cu excepția cazurilor în care această precizare este necesară pentru a exclude orice echivoc.	**Se acceptă** Subpct. 28.1. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.

	74	La pct. 30 cuvintele „ar trebui refuzată” se vor substitui cu cuvintele „se refuză”.	**Se acceptă** Pct. 31. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.
	75	La pct. 41 se va preciza la care agenție se face referință.	**Se acceptă** A se vedea argumentarea la obiecția cu nr. 82.
	76	Cu referire la pct. 64, procedura privind căutarea automatizată în evidențele poliției urmează a fi corelată cu art. 21 din proiectul legii privind cooperarea polițienească internațională. Astfel, proiectul hotărârii nu reflectă condiția prevăzută la alin. (1), potrivit căreia căutările pot fi efectuate în legătură cu infracțiuni sancționate, conform legislației statului solicitant, cu pedeapsa închisorii mai mare de un an.	**Se acceptă** Pct. 66. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.
	77	Totodată, textul „persoane urmărite, dispărute sau implicate în activități infracționale” nu corespunde categoriilor de persoane prevăzute expres la art. 21 alin. (2), respectiv persoanele reținute, bănuite, învinuite și condamnate, motiv pentru care se va revizui.	**Se acceptă** Pct. 66. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.
	78	La pct. 73 se va revedea prevederea propusă, deoarece nu are caracter normativ.	**Se acceptă** Prevederile fostului pct. 73 excluse.
	79	La pct. 90 cuvintele „protecția datelor” se vor substitui cu cuvintele „protecția datelor cu caracter personal”.	**Se acceptă** A se vedea argumentarea la obiecția cu nr. 40.
	80	La pct. 103, cuvintele „revizuirea periodică” se va corela cu art. 48 alin. (2) din proiectul legii, care impune verificarea anuală a înregistrărilor și a activităților de prelucrare.	**Se acceptă** Pct. 104. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.
	81	La pct. 107, din sintagma „legislația în vigoare”, cuvintele „în vigoare” se vor exclude, ca fiind inutile. Regula generală este că referințele la actele normative reprezintă referințe la legislația în vigoare și doar pentru excepțiile de la regulă se va specifica dacă este vorba despre legislația aplicabilă la un anumit moment (obiecție valabilă și pentru pct. 40 din anexa nr. 2).	**Se acceptă** Proiectul ajustat prin: - modificarea pct. 108. din Anexa nr. 1 a proiectului hotărârii de Guvern; - modificarea pct. 40. din Anexa nr. 2 a proiectului hotărârii de Guvern.
	82	La pct. 109 și 110, se remarcă faptul că, stabilirea faptelor care constituie contravenții ori infracțiuni, precum și a condițiilor de angajare a răspunderii juridice, se realizează exclusiv prin lege, neputând fi instituită în mod autonom printr-un act normativ subordonat legii. Prin urmare, norma se va limita la prevederea că încălcarea dispozițiilor Regulamentului atrage răspunderea în condițiile legislației. Observația dată este valabilă și pentru pct. 41 și 42 din anexa nr. 2.	**Se acceptă** Proiectul a fost ajustat prin: - modificarea actualului pct. 109. din Anexa nr. 1 a proiectului hotărârii de Guvern;

			- excluderea pct. 110. din Anexa nr. 1 a proiectului hotărârii de Guvern (care prevedeau răspunderea juridică); - modificarea actualului pct. 40. din Anexa nr. 2 a proiectului hotărârii de Guvern; - excluderea pct. 41 și pct. 42. din Anexa nr. 2 a proiectului hotărârii de Guvern (care prevedeau răspunderea juridică).
	83	***La Regulamentul de organizare și funcționare a Punctelor Naționale de Contact în scopul schimbului de date și informații:*** La pct. 8, se va examina oportunitatea substituirii cuvintelor „expert calificat” cu cuvintele „membru calificat al personalului” sau „specialist calificat”. Or, potrivit Legii nr. 68/2016 cu privire la expertiza judiciară și statutul expertului judiciar, calitatea de expert judiciar și activitatea de expertiză judiciară au un regim juridic distinct, în timp ce verificarea manuală a concordanțelor reprezintă o operațiune tehnică de validare a datelor. Totodată, Regulamentul (UE) 2024/982 (Prüm II) utilizează noțiunea „membru calificat al personalului”, ceea ce impune delimitarea terminologică a acestei activități de atribuțiile specifice expertului judiciar (valabil și pentru pct. 45).	**Se acceptă** A se vedea argumentarea la obiecția cu nr. 18.
	84	La pct. 31 cuvintele „Punctele Naționale de Contact” se vor substitui cu abrevierea PNC.	**Se acceptă** Pct. 31. din Anexa nr. 2 a proiectului hotărârii de Guvern modificat.
	85	La pct. 55, atribuțiile Inspectoratului General de Carabinieri urmează a fi revizuite, întrucât extinderea schimbului de date și informații asupra depistării și investigării infracțiunilor excede atribuțiile stabilite la art. 22 din Legea nr. 219/2018 cu privire la Inspectoratul General de Carabinieri, care nu conferă acestei autorități atribuții de investigare a infracțiunilor. Totodată, soluția nu este corelată cu art. 28 alin. (1) din proiectul de lege privind cooperarea polițienească internațională, care limitează schimbul respectiv la prevenirea infracțiunilor și menținerea ordinii și securității publice în contextul evenimentelor majore cu dimensiune transfrontalieră. Prin urmare, norma se va ajusta corespunzător limitelor competențelor stabilite prin actele normative menționate.	**Se acceptă** Pct. 55. din Anexa nr. 2 a proiectului hotărârii de Guvern modificat.
	86	Pct. 58 și 59 urmează a fi comasate, întrucât dublează aceeași obligație privind interoperabilitatea sistemelor IGC și utilizarea standardului UMF.	**Se acceptă** Proiectul a fost ajustat prin:

			- comasarea punctelor inițiale cu nr. 58 și 59 în noul pct. 58. din Anexa nr. 2 a proiectului hotărârii de Guvern; - excluderea Secțiunii nr. 2 din Capitolul IX care includea punctele inițiale 58 și 59 din Anexa nr. 2 a proiectului hotărârii de Guvern (cu privire la canalele de comunicare).
	87	La pct. 64, accesul la datele proprietarilor de vehicule va fi condiționat de respectarea art. 15 alin. (3) din proiectul legii privind cooperarea polițienească internațională, potrivit căruia asemenea căutări sunt permise exclusiv în privința bănuiților, învinuiților, inculpaților și condamnaților.	**Se acceptă** Pct. 64. din Anexa nr. 2 a proiectului hotărârii de Guvern modificat.
Procuratura Generală (nr. 4-1d/26 din 10.06.2026)	**88**	Proiectul de hotărâre cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații (în continuare – proiect de hotărâre) transpune parțial principalele instrumente europene în materie, inclusiv Regulamentul (UE) 2024/982 (Prüm II), Directiva (UE) 2023/977 privind schimbul de informații dintre autoritățile de aplicare a legii și Decizia 2008/615/JAI. Subsecvent, proiectul prenotat reprezintă un pas important în armonizarea cadrului normativ național cu standardele Uniunii Europene, contribuind la eficientizarea cooperării polițienești internaționale și la consolidarea capacităților de combatere a criminalității transfrontaliere. În speță, din perspectiva atribuțiilor constituționale ale procurorului și a exigențelor procesului penal, considerăm necesară examinarea proiectului prin prisma principiilor fundamentale care guvernează schimbul de informații între autoritățile competente, printre care principiile disponibilității informațiilor, accesului echivalent, confidențialității, proprietății asupra datelor (*originator control principle*), principiul fiabilității datelor. Per ansamblu, proiectul este în mare măsură compatibil cu cele cinci principii fundamentale ale schimbului de informații din acquis-ul UE, cele mai sensibile aspecte fiind accesul echivalent și proprietatea asupra datelor, unde ar fi recomandabilă introducerea unor formulări mai explicite pentru a evita interpretări divergente în practică.	**Se acceptă** Principiile fundamentale (*disponibilitatea, accesul echivalent, confidențialitatea, originator control și fiabilitatea*) au fost integrate în art. 4 din *Legea nr. 209/2026 privind cooperarea polițienească internațională* și detaliate în proiectul hotărârii de Guvern ce vine în implementarea acestei legi.
	89	Astfel, pentru asigurarea respectării depline a principiului accesului echivalent (care presupune că autoritățile altor state membre nu trebuie să fie supuse unor condiții mai restrictive decât autoritățile naționale atunci	**Se acceptă** Cadrul normativ actual reflectă solicitarea dumneavoastră prin faptul că

		când solicită informații), este necesar ca eventualele limitări sau condiții suplimentare aplicabile autorităților străine să fie justificate exclusiv de cerințele naționale privind protecția datelor, secretul urmării penale sau securitatea națională și să nu creeze bariere disproporționate în schimbul de informații.	accesul echivalent este regula, iar orice abatere sau condiție suplimentară este limitată strict la protecția ordinii publice, securității naționale și a drepturilor fundamentale, fiind supusă unor proceduri de control și jurnalizare pentru a asigura proporționalitatea.
	90	În raport cu principiul proprietății asupra datelor considerăm oportună introducerea unei prevederi exprese potrivit căreia informațiile obținute de la o autoritate străină nu pot fi retransmise unei alte autorități fără acordul prealabil al furnizorului inițial, cu excepția cazurilor expres prevăzute de lege.	**Se acceptă** Prevederea este deja inclusă în mod expres la Art. 4 alin. (1) lit. e) și Art. 46 alin. (9) din *Legea nr. 209/2026 privind cooperarea polițienească internațională*. În Regulamentul PUC (Anexa nr. 1), aceasta este corelată cu motivele de refuz (subpct. 28.7), iar nerespectarea principiului atrage răspunderea conform legislației în vigoare, conform trimiterii generale din secțiunea dedicată răspunderii juridice (pct. 109 din Anexa nr. 1, precum și pct. 40 din Anexa nr. 2). Statutul de retransmitere rămâne condiționat exclusiv de acordul prealabil al furnizorului inițial.
	91	Subsecvent, cu referire la principiul fiabilității datelor, considerăm necesară introducerea unei obligații explicite de notificare a tuturor destinatarilor datelor (autorități naționale beneficiare), care au utilizat date declarate ulterior inexacte sau retrase, astfel încât acestea să poată evalua impactul asupra procedurilor penale aflate în desfășurare.	**Se acceptă** Principiul fiabilității, exactității și actualizării datelor este deja consacrat la art. 4 alin. (1) lit. f) din *Legea nr. 209/2026 privind cooperarea polițienească internațională*, care impune informarea fără întârziere a destinatarului în cazul rectificării sau ștergerii datelor. Totodată, pct. 97 din Anexa nr. 1 la PHG stabilește obligația PUC de a notifica imediat autoritatea destinatară despre inexactitatea datelor, acesta fiind modificat în baza obiecției date.
	92	**1. Cu referire la proiectul de hotărâre.**	**Se acceptă** Proiect ajustat, prin:

Serviciul Tehnologia Informației și Securitatea Cibernetică (nr. 1.4/1079/26 din 10.06.2026)		Punctul 1 sintagma „sau, după caz, pentru asigurarea conectivității tehnice securizate necesare schimbului de date” se va exclude. Totodată se va exclude și subpct. 1.6 întrucât STISC nu are calitatea de Punct Național de Contact pe domeniu de competență pentru furnizarea datelor de referință sau a informațiilor necesare schimbului de date. Rolul STISC privind asigurarea conectivității tehnice securizate la rețeaua TESTA este reglementat prin Hotărârea Guvernului nr. 65/2026 *cu privire la conectarea Republicii Moldova la rețeaua TESTA*, prin care STISC este desemnat în calitate de punct de conectare la domeniul local la rețeaua de comunicații securizată a Uniunii Europene TESTA. Totodată se constată că deși proiectul pare să atribuie calitatea de PNC tehnic pentru STISC, în anexele la proiect această noțiune este utilizată și cu referire la entități desemnate ca PNC pe domenii de competență. De exemplu în anexa nr. 1 la pct. 44–45 se utilizează noțiunile „Punct Național de Contact tehnic” și „PNC-urile tehnice” (plural) inclusiv cu referire la STI și CTC-EJ iar la pct. 51 se face trimitere la „PNC-urile tehnice responsabile” fără a specifica cine sunt acestea. Totodată la pct. 48 din aceeași anexă STI al MAI este indicat în calitate de „PNC de domeniu” deși proiectul îi atribuie responsabilități tehnice privind EPRIS - inclusiv la Anexa nr. 2 pct. 49 și pct. 52. Această reglementare neuniformă poate genera neclarități privind delimitarea rolului STISC ca punct de conectare la domeniul local la TESTA față de rolul PNC-urilor desemnate pe domenii de date și față de atribuțiile tehnice ale altor entități implicate.	- modificarea pct. 1. din partea dispozitivă a proiectului hotărârii de Guvern; - excluderea subpct. 1.6. din partea dispozitivă a proiectului hotărârii de Guvern; - modificarea pct. 45., pct. 46. și pct. 52. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	93	**Cu referire la regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații (anexa nr. 1).** **La punctul 5:** - **subpct. 5.2** după cuvintele „incidente cibernetice” se va completa cu textul „responsabil de protejarea infrastructurilor tehnologiei informației și comunicațiilor”, în vederea precizării rolului CERT-UE în raport cu infrastructurile informatice ale instituțiilor, organelor și agențiilor Uniunii Europene. Cuvântul „autoritate” se va substitui cu cuvântul „echipă” având în vedere că CERT-UE nu are personalitate juridică proprie ci reprezintă un serviciu interinstituțional de securitate cibernetică al Uniunii Europene, aflat	**Se acceptă** Subpct. 5.2. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.

		administrativ în cadrul Direcției Generale Servicii Digitale a Comisiei Europene (Directorate-General for Digital Services – DG DIGIT).	
	94	**La punctul 5:** - **subpct. 5.8** se va revizui noțiunea „incident semnificativ de securitate cibernetică” întrucât nu rezultă cu claritate dacă definiția propusă vizează „incidentul de securitate” prevăzut la art. 54 alin. (1) din Regulamentul (UE) 2024/982 sau o noțiune specifică Legii nr. 48/2023 privind securitatea cibernetică. Clarificarea este necesară deoarece Regulamentul (UE) 2024/982 utilizează noțiunea de „incident de securitate” în raport cu securitatea Router-ului și a EPRIS, inclusiv pentru evenimente care au sau pot avea impact asupra securității acestora. În schimb, Legea nr. 48/2023 utilizează terminologia specifică securității cibernetice, inclusiv noțiunile de „incident cibernetic”, „incident cibernetic evitat la limită” și „amenințare cibernetică”, fiecare având un conținut juridic separat. Prin urmare, noțiunea urmează a fi clarificată și corelată cu actul normativ avut în vedere, pentru a evita suprapunerea între „incidentul de securitate” în sensul Regulamentului (UE) 2024/982 și noțiunile reglementate de Legea nr. 48/2023.	**Se acceptă** Subpct. 5.8. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.
	95	**La punctul 5:** - **subpct. 5.14** și în tot cuprinsul proiectului se va reanaliza utilizarea noțiunii „S-TESTA” și uniformizarea terminologiei prin utilizarea noțiunii „TESTA”. Potrivit definiției publicate la nivelul Uniunii Europene, TESTA (Trans-European Services for Telematics between Administrations) reprezintă infrastructura paneuropeană securizată, cu disponibilitate ridicată, destinată schimbului de informații sensibile între autoritățile publice, care necesită niveluri garantate de servicii privind rețeaua, performanța și/sau securitatea. În acest context precum și având în vedere că Hotărârea Guvernului nr. 65/2026 utilizează noțiunea „TESTA”, folosirea în prezentul proiect a noțiunii „S-TESTA” poate crea neclarități privind infrastructura vizată.	**Se acceptă** Întregul text al proiectul hotărârii de Guvern adaptat.
	96	**Pct. 14** se va reformula din perspectiva modului de organizare și funcționare al PUC fără indicarea expresă a STISC întrucât secțiunea respectivă reglementează activitatea PUC, nu atribuțiile STISC privind conectivitatea tehnică la rețeaua TESTA.	**Se acceptă** Pct. 15. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.

		În acest sens, se propune următoarea redacție: „14. PUC utilizează conectivitatea tehnică securizată necesară schimbului de date și informații cu infrastructurile externe, asigurată potrivit Hotărârii Guvernului nr. 65/2026 *cu privire la conectarea Republicii Moldova la rețeaua TESTA* și cadrului normativ aplicabil.”.	
	97	**Pct. 35** se va exclude sintagma „de către PNC tehnic (STISC)” din ultima propoziție întrucât în contextul descris atribuirea către STISC a responsabilităților menționate nu este corelată cu rolul stabilit prin Hotărârea Guvernului nr. 65/2026, care vizează punctul de conectare la domeniul local la TESTA și asigurarea conectivității tehnice securizate.	**Se acceptă** Pct. 36. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat.
	98	**La pct. 44** sintagma „administrate tehnic de către Punctul Național de Contact tehnic” urmează a fi revizuită întrucât nu rezultă cu claritate care este autoritatea/instituția publică vizată.	**Se acceptă** Pct. 45. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat în baza obiecției cu nr. 92.
	99	**La pct. 45** ultima propoziție: „Configurarea, mentenanța și securitatea cibernetică a componentelor tehnice ale Router-ului nu cad în sarcina PUC, fiind asigurate de PNC-urile tehnice (STISC, STI, CTC-EJ) conform atribuțiilor din Anexa nr. 2.” se va exclude întrucât prima propoziție a punctului stabilește deja suficient că competența PUC se limitează exclusiv la utilizarea operativă a Router-ului. Menținerea ultimei propoziții poate crea neclarități privind statutul și atribuțiile „PNC-urilor tehnice” mai ales în condițiile în care proiectul utilizează neuniform această noțiune. Totodată, în cazul abrevierii „CTC-EJ”, se recomandă indicarea denumirii complete la prima utilizare, urmată de abrevierea corespunzătoare. De asemenea, abrevierea urmează a fi utilizată uniform în tot cuprinsul proiectului, fie în forma „CTC-EJ”, fie în forma „CTCEJ”, după opțiunea autorului.	**Se acceptă** Pct. 46. din Anexa nr. 1 a proiectului hotărârii de Guvern modificat în baza obiecției cu nr. 92.
	100	**Cu referire la proiectul regulamentului de organizare și funcționare a Punctelor Naționale de Contact în scopul schimbului de date și informații (anexa nr. 2).** **La pct. 2** după cuvântul „autoritățile” se va completa cu cuvintele „/instituțiile publice” având în vedere că unele entități desemnate în calitate de PNC au statut de instituții publice.	**Se acceptă** Pct. 2. din Anexa nr. 2 a proiectului hotărârii de Guvern modificat.
	101	**La pct. 4** formularea introductivă „În sensul prezentului Regulament, se desemnează următoarele autorități în calitate de PNC” se va substitui cu formularea „În sensul prezentului Regulament, sunt PNC următoarele	**Se acceptă** Pct. 4. din Anexa nr. 2 a proiectului hotărârii de Guvern modificat.

		autorități/instituții publice competente”, întrucât desemnarea PNC-urilor este prevăzută în proiectul hotărârii Guvernului, iar anexa nr. 2 urmează să reglementeze modul de organizare și exercitare a atribuțiilor acestora.	
	102	**La pct. 4, subpct. 4.6** se va exclude întrucât rolul STISC urmează a fi reglementat separat de atribuțiile PNC-urilor desemnate pe domenii de competență, prin raportare la Hotărârea Guvernului nr. 65/2026. În acest sens, se propune includerea unei norme separate după pct. 4, cu renumerotarea corespunzătoare a punctelor subsecvente, în următoarea redacție: „5. Serviciul Tehnologia Informației și Securitate Cibernetică (în continuare – STISC) exercită potrivit Hotărârii Guvernului nr. 65/2026 *cu privire la conectarea Republicii Moldova la rețeaua TESTA*, rolul de punct de conectare la domeniul local (Local Domain Connection Point) la rețeaua de comunicații securizată a Uniunii Europene TESTA (Trans-European Services for Telematics between Administrations).”.	**Se acceptă** Proiect ajustat, prin: - excluderea subpct. 4.6. din Anexa nr. 2 a proiectului hotărârii de Guvern (unde STISC a fost desemnat ca punct tehnic de contact); - modificarea pct. 80 din Anexa nr. 2 a proiectului hotărârii de Guvern.
	103	**La pct. 5** sintagma „infrastructura națională de comunicații securizate administrată de către Punctul Național de Contact tehnic (STISC)” se va substitui cu sintagma „infrastructura de comunicații securizată utilizată pentru schimbul de date și informații” întrucât formularea actuală nu este corelată cu terminologia utilizată în Hotărârea Guvernului nr. 65/2026. Potrivit acesteia, STISC este desemnat în calitate de punct de conectare la domeniul local la rețeaua TESTA iar conectarea entităților din Republica Moldova la rețeaua TESTA se realizează conform regulamentului aprobat de STISC.	**Se acceptă** Pct. 5. din Anexa nr. 2 a proiectului hotărârii de Guvern modificat, a se vedea argumentarea la obiecția cu 7.
	104	**Pct. 11 subpct. 11.4** textul se va ajusta conform obiecției formulate la pct. 5 subpct. 5.14 din anexa nr. 1.	**Se acceptă** Întregul text al proiectul hotărârii de Guvern adaptat.
	105	**La Capitolul XII:** - **Secțiunea 1** se va revizui denumirea secțiunii și se va comasa pct. 78 și 79 într-un singur punct întrucât formulările actuale utilizează noțiunea de „PNC tehnic” și atribuie STISC responsabilități formulate prea larg, inclusiv cu referire la administrarea infrastructurii S-TESTA, funcționarea Router-ului UE, a sistemului EPRIS, a sistemului EUCARIS și a interfețelor de acces la Sistemul de Informații Schengen. Or, potrivit Hotărârii Guvernului nr. 65/2026, rolul STISC vizează punctul de conectare la domeniul local la rețeaua TESTA și măsurile de	**Se acceptă** - modificarea pct. 80. din Anexa nr. 2 a proiectului hotărârii de Guvern; - excluderea pct. 79. din Anexa nr. 2 a proiectului hotărârii de Guvern (unde au fost enumerate funcțiile principale ale STISC).

		securitate cibernetică aplicabile entităților conectate la acesta, fără a rezulta că STISC administrează sau asigură funcționarea sistemelor/infrastructurilor utilizate pentru schimbul automatizat de date. Totodată, prevederile proiectului atribuie anumite responsabilități tehnice altor autorități. Astfel, STI al MAI are competențe tehnice în raport cu EPRIS iar pentru Sistemul de Informații Schengen sunt prevăzute atribuții ale ASP privind interfața tehnică și fluxul de date aferent anumitor categorii de alerte. Totodată, ASP are responsabilități legate de conexiunea tehnică a registrelor proprii cu sistemul EUCARIS pentru gestionarea datelor referitoare la mijloacele de transport. Prin urmare, Secțiunea 1 va fi expusă în următoarea redacție: „Secțiunea 1 Atribuțiile specifice în calitate de punct de conectare la domeniul local la rețeaua TESTA **78.** STISC exercită potrivit Hotărârii Guvernului nr. 65/2026 cu privire la conectarea Republicii Moldova la rețeaua TESTA rolul de punct de conectare la domeniul local la rețeaua de comunicații securizată a Uniunii Europene TESTA.”.	
	106	**- Secțiunea a 3-a se vor exclude punctele 82 și 84** întrucât acestea vizează aspecte de organizare internă a STISC precum și obligații de raportare tehnică periodică față de PUC care nu rezultă cu claritate din obiectul de reglementare al prezentului proiect, din rolul STISC stabilit prin Hotărârea Guvernului nr. 65/2026 și nici din Regulamentul (UE) 2024/982.	**Se acceptă** Secțiunea a 3-a din Capitolul XII din Anexa nr. 2 a proiectului hotărârii de Guvern a fost exclusă.
Serviciul de Informații și Securitate (nr. IE/6002 din 12.06.2026)	**107**	Considerăm oportună completarea **pct. 1 din proiectul Hotărârii**, prin includerea Procuraturii Generale în calitate de Punct Național de Contact. Astfel, subliniem faptul că, necesitatea acestei completări derivă din atribuțiile constituționale și legale ale Procuraturii privind conducerea și exercitarea urmăririi penale, cooperarea juridică internațională în materie penală și coordonarea activităților de investigare a infracțiunilor grave, inclusiv a infracțiunilor de terorism și a infracțiunilor conexe acestora. Respectiv, consemnăm că, implicarea Procuraturii Generale în calitate de Punct Național de Contact va contribui la asigurarea legalității schimbului de informații aferente cauzelor penale și va evita riscul transmiterii unor informații procesul-penale prin intermediul unor autorități care nu dețin competențe procesuale corespunzătoare.	**Nu se acceptă** Propunerea este respinsă deoarece Procuratura Generală nu administrează baze de date de referință, necesare schimbului automatizat de date și informații și nu deține infrastructura tehnică ori conectivitatea la rețeaua securizată TESTA (administrată de STISC) pentru a asigura interfața tehnică cerută unui PNC. Atribuțiile procesuale ale PG sunt deja garantate prin procedurile de autorizare judiciară și supraveghere a legalității prevăzute în Regulamentul PUC și în Legea nr.

			209/2026 privind cooperarea polițienească internațională.
	108	Consecvent, în contextul expus supra, propunem completarea proiectului cu prevederi potrivit cărora schimbul de informații și date aferente cauzelor penale, în care obiectul investigației îl constituie infracțiunile de terorism sau infracțiunile conexe terorismului, să fie realizat prin intermediul Procuraturii Generale. Prin urmare, completarea propusă este necesară pentru o delimitare clară dintre activitățile de prevenire și identificare timpurie a riscurilor teroriste și activitățile procesual-penale desfășurate în cadrul urmăririi penale, precum și pentru asigurarea respectării normelor Codului de procedură penală, referitoare la gestionarea și transmiterea informațiilor aferente cauzelor penale.	**Se acceptă** Proiectul reglementează mecanismele de cooperare polițienească internațională și de schimb de date și informații între autoritățile competente, fără a aduce atingere competențelor procesual-penale ale organelor de urmărire penală și ale procurorului, exercitate în condițiile Codului de procedură penală. Totodată, atribuțiile Procuraturii Generale în cadrul procesului penal, inclusiv cele privind autorizarea, conducerea și controlul urmăririi penale, sunt garantate de legislația procesual-penală și de *Legea nr. 209/2026 privind cooperarea polițienească internațională*. În acest context, desemnarea Procuraturii Generale drept canal distinct pentru schimbul internațional de date și informații aferente cauzelor penale nu este necesară și nu corespunde arhitecturii instituționale a mecanismului PUC/PNC instituit prin proiect.
	109	De asemenea, considerăm necesară completarea **pct. 1.5 din proiectul Hotărârii** și a normelor operaționale aferente (**pct. 4.5 din Anexa nr. 2**) cu precizarea expresă a faptului că, Serviciul de Informații și Securitate furnizează informațiile necesare prevenirii infracțiunilor teroriste în condițiile, limitele și conform procedurilor prevăzute de legislația națională. Prin urmare, datele și informațiile relevante obținute anterior pornirii urmării penale sau în cadrul activităților de identificare, documentare și investigare a faptelor susceptibile de a constitui infracțiuni de terorism urmează a fi furnizate de către Serviciu, cu respectarea regimului juridic aplicabil informațiilor operative, informațiilor atribuite la secret de stat și/sau surselor specifice de informații.	**Se acceptă** Proiect ajustat, prin: - modificarea subpct. 1.5. din clauza de adoptare a PHG; - modificarea subpct. 4.5. din Anexa nr. 2 a proiectului hotărârii de Guvern.
	110	**În Anexa nr. 1 (*pct. 10.10, pct. 34 și pct. 35*)**, precum și în **Anexa nr. 2 (*Cap. IX, pct. 72-77*)**, propunem revizuirea regimului de accesibilitate a	**Se acceptă** Proiect ajustat, prin:

		informațiilor gestionate de Serviciul de Informații și Securitate, prin încadrarea acestora în categoria **informațiilor indirect accesibile** (*conform pct. 5.11 din Anexa nr.1*). În acest sens, furnizarea informațiilor respective urmează să se realizeze exclusiv în baza solicitărilor individuale adresate Serviciului, cu evaluarea prealabilă a legalității și oportunității divulgării acestora, fără instituirea unui acces direct și permanent la sistemele informaționale administrate/operate de către Serviciu. În aceeași ordine de idei, considerăm absolut indispensabilă revizuirea prevederilor menționate, în vederea excluderii oricăror interpretări/neclarități care reglementează permiterea accesului direct la bazele de date și/sau la sistemele informaționale ale Serviciului, prin stabilirea expresă a faptului că accesul la informațiile gestionate de Serviciul de Informații și Securitate se realizează exclusiv prin mecanismul solicitare-răspuns, fără posibilitatea interconectării directe a bazelor de date operaționale ale Serviciului sau acordarea accesului tehnic direct la sistemele informaționale administrate de acesta.	- modificarea subpct. 1.5. din clauza de adoptare a PHG; - modificarea subpct. 5.11. din Anexa nr. 1 a proiectului hotărârii de Guvern; - modificarea subpct. 4.5. din Anexa nr. 2 a proiectului hotărârii de Guvern; - includerea noului pct. 74. în Anexa nr. 2 a proiectului hotărârii de Guvern.
	111	Suplimentar, se propune completarea proiectului cu norme/garanții suplimentare privind protecția informațiilor secretizate, prin instituirea principiului potrivit cărora schimbul de date și informații nu poate aduce atingere regimului juridic aplicabil informațiilor atribuite la secretul de stat. De asemenea, considerăm oportună reglementarea expresă a dreptului autorității furnizoare de a refuza transmiterea informațiilor sau de a limita volum acestora în situațiile în care transmiterea acestora poate compromite activități operative în curs, surse de informații, metode și mijloace specifice de activitate sau pot aduce atingere intereselor de securitate națională a Republicii Moldova.	**Se acceptă** Garanțiile solicitate sunt acoperite de textul actual al proiectului hotărârii de Guvern prin prevederile subpct. 7.5., subpct. 21.1. și subpct. 28.3. din Anexa nr. 1, precum și pct. 79 din Anexa nr. 2 a proiectului hotărârii de Guvern.
Cancelaria de Stat (mențiune pe e-Legiferare)	**112**	Direcția managementul funcției publice a examinat proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului schimbului de date și informații, și în limita competențelor funcționale recomandă înlocuirea termenului de subdiviziune structurală în termenul subdiviziune internă, la pct.47, pct.70, precum și pe parcursul textului proiectului, în conformitate cu Normele privind instituirea subdiviziunilor interne ale autorității publice din Anexa nr.12 a H.G. nr.201/2009.	**Se acceptă** Proiectul a fost ajustat prin: - modificarea pct. 46. și pct. 71. din Anexa nr. 2 a proiectului hotărârii de Guvern.

Ministerul Dezvoltării Economice și Digitalizării (nr. 03-1964 din 10.06.2026)	**113**	Lipsa obiecțiilor și propunerilor.	**S-a luat act**
PROCEDURA DE NOTIFICARE/EXPERTIZARE			
Centrul Național Anticorupție (nr. 06/2/12587 din 14.07.2026 Raport de expertiză nr. EHG26/11685 din 14.07.2026)	**114**	**Pct.1, anexa nr.2 potrivit proiectului hotărârii de Guvern** **Obiecții:** Analiza normelor citate relevă că, deși prevederile propuse transpun Directiva (UE) 2023/977 privind schimbul de informații dintre autoritățile de aplicare a legii ale statelor membre, nu sunt reglementate mecanismele prin care Centrul Național Anticorupție va participa efectiv la schimbul de informații. Desemnarea exclusivă a Centrului tehnico-criminalistic și expertize judiciare al Inspectoratului General al Poliției, Serviciului Tehnologii Informaționale, Inspectoratului General de Carabinieri, Agenție i Servicii Publice și Serviciului de Informații și Securitate ca Puncte Naționale de Contact (PNC), cu omiterea Centrului Național Anticorupție (CNA), concentrează nejustificat gestionarea fluxurilor de date operative internaționale la nivelului Inspectoratului General al Poliției (IGP), prin Punctul Unic de Contact (PUC). O asemenea abordare elimină independența funcțională a CNA, instituind un mecanism indirect de filtrare a datelor și o dependență instituțională contrară specificului activității de combatere a corupției. Obligarea CNA de a solicita informații operative (inclusiv prin SIENA) exclusiv prin intermediul PUC gestionat de IGP anulează confidențialitatea investigațiilor. Mai mult, privarea CNA de statutul de PNC operațional, deși instituția utilizează deja în mod direct două canale securizate SIENA, constituie o restricționare nejustificată a capacităților tehnice și operaționale existente. În același context, punctul 36 din anexa nr. 1 din proiect stabilește cerințele operaționale privind conectarea PNC-urilor la aplicația securizată SIENA - *„PUC, precum și toate PNC-urile care ar putea fi implicate în schimbul de informații, sunt conectate direct la aplicația securizată SIENA, inclusiv, după caz, prin dispozitive mobile securizate [...]”* ori în situația dacă CNA nu va fi înregistrat drept PNC există riscul de a nu avea accesul necesar pentru schimbul de date prin această platformă.	**Se acceptă parțial** Legea nr. 209/2026 privind cooperarea polițienească internațională, în calitatea sa de act primar, stabilește la art. 6 alin. (2) o listă limitativă de domenii (ADN, dactiloscopie, vehicule, imagini faciale, evidențe polițienești, terorism) pentru care Guvernul poate desemna Puncte Naționale de Contact. Este imperativ de menționat că aceste domenii survin strict din transpunerea actelor Uniunii Europene enumerate în preambulul proiectului Hotărârii de Guvern — în special Regulamentul (UE) 2024/982 (Prüm II), Deciziile 2008/615/JAI și 2008/616/JAI, precum și Directiva (UE) 2023/977 — care definesc cadrul tehnic și categoriile de date supuse schimbului automatizat la nivel european. Mandatul specializat al CNA (corupția) nu este prevăzut ca un domeniu distinct de sine stătător pentru un PNC în arhitectura legii, iar proiectul Hotărârii de Guvern , fiind un act subordonat, nu poate adăuga domenii noi de competență care nu se regăsesc în textul actului normativ de rang superior. Categoriile de date gestionate de CNA (informații financiare, economice) sunt deja incluse în obiectul schimbului de informații conform art. 2 alin. (4) lit. f) din Legea nr. 209/2026 privind

		Prin urmare, se consideră necesară completarea listei autorităților în calitate de Puncte Naționale de Contact cu CNA, completare care va transforma CNA într-un Punct Național de Contact și îi va conferi un statut expres de autoritate responsabilă de schimbul de date pe domeniul de competență. **Recomandări:** În vederea asigurări unei reglementări clare și aplicabile în practică, care să garanteze implicarea efectivă a Centrului Național Anticorupție în mecanismul de cooperare și schimb de informații cu autoritățile de aplicare a legii din statele Uniunii Europene, cu respectarea competențelor conferite de legislația națională, recomandăm următoarele modificări: 1. La punctul 1 din proiectul hotărârii de Guvern, acesta se propune de completat cu subpunctul 1.6. care va avea următorul cuprins: *„1.6. Centrul Național Anticorupție – pentru domeniul prevenirii, depistării, investigării și urmăririi infracțiunilor de corupție, a actelor conexe corupției, a celor cu caracter financiar și a altor infracțiuni atribuite în competența sa, precum și în domeniul recuperării bunurilor infracționale, prin furnizarea și primirea informațiilor necesare în regim direct și indirect, în limitele și conform procedurilor prevăzute de legislația națională.”* 2. La punctul 4 din anexa nr.2 potrivit proiectului, acesta se propune de completat cu subpunctul 4.6. care va avea următorul cuprins: *„4.6. Centrul Național Anticorupție – pentru domeniul prevenirii, depistării, investigării și urmăririi infracțiunilor de corupție, a actelor conexe corupției, a celor cu caracter financiar și a altor infracțiuni atribuite în competența sa, precum și în domeniul recuperării bunurilor infracționale, prin furnizarea și primirea informațiilor necesare în regim direct și indirect, în limitele și conform procedurilor prevăzute de legislația națională.”* 3. În același context, se propune completarea Regulamentului de organizare și funcționare a Punctelor Naționale de Contact în scopul schimbului de date și informații (anexa nr.2 potrivit proiectului) cu un capitol care va prevedea competențele legale ale Centrul Național Anticorupție și rolului acestuia în schimbul de informații cu autoritățile de aplicare a legii din Uniunea Europeană, după cum urmează: *„XII. Centrul Național Anticorupție*	cooperarea polițienească internațională. Desemnarea CNA ca PNC ar crea o fragmentare excesivă a infrastructurii tehnice naționale. Rolul de „Punct Național de Contact” implică administrarea tehnică a nodurilor de interconectare cu UE (Router, EPRIS), în timp ce participarea CNA la schimbul de date este pe deplin garantată prin calitatea sa de „*autoritate competentă de aplicare a legii*”, care poate utiliza canalul SIENA și interfața PUC/SPOC fără a fi necesar statutul de administrator tehnic de domeniu. Faptul că Centrul Național Anticorupție a obținut deja de la Europol un „*full private account*” pe canalul securizat SIENA, reprezintă un aspect de ordin tehnic și operațional care nu va fi afectat de aprobarea prezentului proiect. Utilizarea acestuia rămâne o prioritate implicită pentru schimburile cu partenerii UE și Europol. În calitate de „autoritate de aplicare a legii desemnată”, CNA își păstrează dreptul de a utiliza direct canalele securizate conform competențelor sale. Statutul de PNC vizat de proiect se referă strict la administrarea tehnică a nodurilor naționale de date (Router UE, EPRIS), sarcini distincte de operarea curentă a mesageriei SIENA. Integrarea CNA în noul mecanism presupune doar obligația transmiterii unei copii a cererilor către PUC pentru triaj și prevenirea suprapunerii investigațiilor. Astfel, proiectul nu restrânge accesul tehnic existent, ci doar asigură trasabilitatea națională a fluxurilor de date fără a aduce

		Secțiunea 1 Atribuțiile specifice în domeniul prevenirii și investigării infracțiunilor atribuite în competența CNA și în scopul recuperării bunurilor infracționale *80. Centrul Național Anticorupție este desemnat în calitate de PNC responsabil pentru domeniul prevenirii, depistării și investigării infracțiunilor de corupție și a altor infracțiuni aflate în competența sa, precum și în scopul recuperării bunurilor infracționale, în cadrul mecanismului de schimb de informații (furnizare/solicitare) aferente acestui domeniu. În exercitarea acestor atribuții, Centrul Național Anticorupție furnizează direct sau indirect prin PUC datele și informațiile necesare schimbului internațional de informații, exclusiv în baza mecanismului solicitare-răspuns, fără acordarea unui acces tehnic direct sau permanent la sistemele informaționale proprii.* *81. Activitatea PNC din cadrul Centrului Național Anticorupție se desfășoară cu respectarea independenței operaționale, fără a aduce atingere competențelor sale prevăzute de legislația specială, cu respectarea principiilor legalității, necesității, proporționalității și confidențialității.* *Secțiunea a 2-a Standarde tehnice și canale de comunicare* *82. Centrul Național Anticorupție în calitate de PNC va utiliza pentru schimbul de informații (furnizare/solicitare) canalul securizat SIENA, în condițiile legislației naționale și ale standardelor Uniunii Europene. Rolul PUC în acest proces este limitat la asigurarea schimbului operativ de informații și a interfeței tehnice de comunicație, fără a deține competențe de coordonare, analiză sau intervenție în domeniile aflate în competența Centrului Național Anticorupție, care rămân în responsabilitatea exclusivă a acestuia.* *83. Pentru transmiterea solicitărilor de informații, a răspunsurilor și a informațiilor furnizate din proprie inițiativă, precum și pentru acțiunile ulterioare confirmării unei concordanțe (hit), Centrul Național Anticorupție utilizează ca interfață principală de comunicare canalul SIENA sau alte canale securizate de cooperare internațională, în condițiile prevăzute de legislația națională și de acordurile bilaterale aplicabile. În cazuri urgente, care impun prevenirea unui risc iminent pentru desfășurarea unei investigații sau pentru recuperarea bunurilor provenite din infracțiuni, Centrul Național Anticorupție colaborează cu PUC pentru urgentarea schimbului de informații.*	atingere independenței operaționale a instituției. Dat fiind faptul că proiectul de Lege (deja transmis spre coordonare externă în adresa Comisiei Europene) nu a prevăzut CNA printre autoritățile de bază pentru pilonii tehnici Prüm II, includerea acestuia în proiectul hotărârii de Guvern cu statut de PNC ar reprezenta o excedare a normei de împuternicire. Aceasta ar vulnerabiliza actul sub aspectul legalității, încălcând principiul conform căruia actul secundar nu poate modifica sau extinde sfera de aplicare a actului primar. De asemenea se atrage atenția la faptul că proiectul hotărârii de Guvern este un act normativ de executare a legii. Având în vedere că proiectul de lege, transmis deja Comisiei Europene spre coordonare externă, nu desemnează Centrul Național Anticorupție printre autoritățile competente pentru pilonii tehnici Prüm II, includerea acestuia în proiectul hotărârii Guvernului în calitate de Punct Național de Contact nu poate fi susținută. Proiectul hotărârii Guvernului are caracter subsecvent și urmărește asigurarea implementării prevederilor proiectului de lege, inclusiv a cadrului instituțional și a mecanismelor de cooperare stabilite de acesta, fără a putea completa sau extinde categoria autorităților desemnate prin actul normativ primar. În vederea cooperării la nivel național pentru asigurarea, a fost inclus un nou

		Secțiunea a 3-a Securitatea informațiilor, jurnalizarea și raportarea *84. Centrul Național Anticorupție desemnează nominal, prin act administrativ, persoanele responsabile de executarea atribuțiilor în cadrul PNC, autorizate să efectueze interogările și să gestioneze fluxul de date.* *85. Centrul Național Anticorupție este responsabil de securitatea fizică și informațională a bazelor de date și a sistemelor informaționale proprii, asigurând autentificarea utilizatorilor autorizați, controlul accesului, jurnalizarea operațiunilor și implementarea măsurilor tehnice și organizatorice necesare pentru protecția informațiilor și a datelor cu caracter personal, în conformitate cu legislația națională.* *86. Schimbul de date și informații efectuat de Centrul Național se realizează cu respectarea regimului juridic aplicabil informațiilor operative, informațiilor atribuite la secret de stat, datelor cu caracter personal și altor informații cu accesibilitate limitată, în condițiile și limitele prevăzute de legislația națională. Mecanismul de schimb de date și informați i instituit conform prezentului act normativ, nu obligă Centrul Național Anticorupție să divulge informații a căror comunicare este interzisă sau restricționată prin lege ori care ar putea prejudicia desfășurarea activităților speciale de investigații, a urmăririi penale, a procesului de identificare, indisponibilizare și recuperare a bunurilor infracționale sau îndeplinirea altor atribuții prevăzute de lege.”* Pe cale de consecință, Capitolul XII din proiect devine Capitolul XIII, cu renumerotarea corespunzătoare a punctelor următoare.	punct în preambulul proiectului hotărârii de Guvern, cu următorul cuprins: „ **3.** *Autoritățile competente de aplicare a legii care exercită atribuții în domeniul activității speciale de investigații, organele de urmărire penală, precum și alte autorități naționale relevante care dețin informații relevante pentru prevenirea, depistarea sau investigarea infracțiunilor, inclusiv informații indirect accesibile, au obligația de a coopera activ cu Punctul Unic de Contact, de a acorda suportul necesar și de a furniza, fără întârzieri nejustificate, datele și informațiile solicitate în vederea asigurării îndeplinirii sarcinilor Punctului Unic de Contact prevăzute de prezenta hotărâre.*”.
	115	**Pct.11 subpct.11.10. din anexa nr.1 potrivit proiectului hotărârii de Guvern** **Obiecții:** În formula propusă de autor, utilizarea în textul normei citate a termenului „personal desemnat”, fără indicarea clară a apartenenței instituționale a acestuia, oferă conducătorilor autorităților publice o putere discreționară nejustificată. În lipsa unei precizări exprese, textul este lipsit de claritate, nefiind previzibil dacă prevederea se referă exclusiv la personalul Punctelor Naționale de Contact (PNC) sau dacă include și personalul altor autorități de aplicare a legii care, potrivit competențelor legale, cooperează cu Europol și participă la schimbul internațional de	**Se acceptă** Proiectul a fost ajustat prin: - modificarea subpct. 11.10. al pct. 11. din Anexa nr. 1 a proiectului hotărârii de Guvern.

		informații. O asemenea formulare defectuoasă generează interpretări neuniforme și dificultăți în aplicarea practică a normei. O normă neclară poate fi utilizată în mod abuziv pentru a restricționa artificial accesul ofițerilor de investigații din cadrul altor autorități de aplicare a legii la bazele de date. Această barieră instituțională poate admite protejarea unor grupuri sau rețele infracționale, prin limitarea capacității de monitorizare și prin controlul selectiv ori blocarea informațiilor transmise către Europol. Prin urmare, având în vedere că schimbul de informații cu Europol nu se realizează exclusiv prin intermediul personalului PNC, ci implică în mod direct persoane desemnate din cadrul altor autorități de aplicare a legii, se impune individualizarea expresă a beneficiarilor acestui drept de acces. Luând în considerare că normele care reglementează accesul la date cu caracter personal, secret de stat sau informații operative trebuie să fie precise, previzibile și limitative, neindividualizarea subiecților autorizați creează un vid normativ care riscă să favorizeze interpretările neuniforme și diminuarea responsabilității în cazul utilizării abuzive sau frauduloase a datelor. Astfel, specificarea clară a categoriilor de personal instituie un mecanism transparent de control a accesărilor. În caz contrar, incertitudinea cu privire la subiecții autorizați limitează capacitatea de identificare a eventualelor scurgeri de informații sau accesări neautorizate, generând impunitatea în fața unor potențiale acte de corupție. **Recomandări:** Recomandăm completarea cuvintelor *„personalului desemnat”* cu textul *„din cadrul PNC sau alte autorități de aplicare a legii,”*.	
	116	**Pct.20 din anexa nr.1 potrivit proiectului hotărârii de Guvern** **Obiecții:** Mecanismul propus prin expresia *„transmite o cerere [...] direct unei autorități competente dintr-un alt stat”* nu este corelat cu celelalte instrumente și proceduri reglementate în textul proiectului. Noțiunea de *„cereri directe”* nu beneficiază de o definiție sau de o delimitare conceptuală clară în textul proiectului. În lipsa unor precizări exprese, norma va genera interpretări abuzive și aplicări neuniforme în practică. Nu este clar dacă această procedură vizează schimbul de informații realizat în baza	**Nu se acceptă** Norma prevăzută la pct. 20 reprezintă o transpunere obligatorie a Art. 6 din Directiva (UE) 2023/977 a Parlamentului European și a Consiliului. Scopul acestei prevederi este de a permite PUC să își exercite funcția de coordonare strategică și triaj, esențială pentru prevenirea suprapunerii investigațiilor la nivel internațional și național.

		acordurilor bilaterale, cooperarea prin canale oficiale consacrate (Interpol, Europol, SELEC etc.) sau alte forme de cooperare instituțională existente. Un alt aspect, obligația corelativă de a transmite simultan copii ale cererilor și informațiilor atât către PUC național, cât și către punctul unic de contact al statului partener, excedează bunele practici și mecanismele de cooperare internațională. Cooperarea internațională dintre autoritățile competente se desfășoară prin canale oficiale consacrate de tratatele internaționale, acordurile bilaterale și legislația națională, iar fiecare autoritate poartă răspundere pentru corespondența pe care o inițiază în limitele competențelor sale. Transmiterea automată a tuturor copiilor schimburilor de informații operative către PUC poate conduce la o multiplicare nejustificată a fluxurilor de date, implicit a celor cu caracter personal și a datelor de investigație. Acest fapt sporește riscul de scurgere a informațiilor sensibile și de încălcare a regimului secretului de stat. Totodată, nu este justificată necesitatea colectării și stocării acestor copii, în condițiile în care punctul 38.4 din proiect prevede că datele sunt supuse reexaminării periodice și ștergerii după cel mult 6 luni de la încheierea schimbului de informații. În aceste condiții, obligația de transmitere a copiilor tuturor cererilor și informațiilor apare ca fiind disproporționată în raport cu scopul urmărit și contravine practicii generale de corespondență și schimb de informații dintre autoritățile competente, fiind întemeiată pe comunicarea directă prin canalele de cooperare stabilite de legislația aplicabilă și de acordurile internaționale sau bilaterale. **Recomandări:** Recomandăm excluderea punctului 20 din proiect sau, după caz, reformularea acestuia astfel încât obligația de informare a PUC să fie limitată la cazurile expres prevăzute de lege sau la situațiile în care coordonarea prin PUC este necesară.	Transmiterea copiei simultane este singura modalitate prin care PUC poate asigura corelarea automată a cazurilor internaționale cu dosarele de investigație naționale, prin intermediul Sistemului electronic unic de gestionare a cazurilor. Aceasta garantează că resursele statului sunt utilizate eficient și că nu există interpelări divergente pe același subiect. Temerile privind scurgerea informațiilor sensibile sunt acoperite prin derogările prevăzute la pct. 21, care permit autorităților să nu informeze PUC în cazuri de terorism, investigații extrem de sensibile sau când este în pericol siguranța unei persoane. Astfel, principiul confidențialității este protejat fără a sacrifica arhitectura SPOC impusă de UE. Toate copiile transmise către PUC sunt supuse acelorași rigori de jurnalizare și securitate multifactorială prin rețeaua TESTA și aplicația SIENA. Mai mult, proiectul prevede obligația de reexaminare și ștergere a datelor care nu mai sunt necesare după cel mult 6 luni, limitând astfel riscul stocării nejustificate. Pentru a elimina ambiguitatea privind noțiunea de „*cereri directe*”, textul pct. 20 din Anexa nr.1 a fost completat cu o trimitere expresă la art. 6 alin. (5) din Legea nr. 209/2026 privind cooperarea polițienească internațională. Această modificare ancorează norma din proiectul de Hotărâre de Guvern în actul normativ de rang superior, care permite autorităților competente să realizeze schimbul de date „în mod direct... prin

			canalele de comunicare securizate avute la dispoziție”. În concluzie, excluderea normei prevăzute la pct. 20 din Anexa nr. 1 ar atrage după sine un risc major de declanșare a procedurii de constatare a neîndeplinirii obligațiilor (infringement) din partea Comisiei Europene pentru neconformitatea cu Directiva 2023/977 și ar priva PUC de instrumentul esențial pentru coordonarea cooperării polițienești internaționale.
	117	**Pct.22 din anexa nr.1 potrivit proiectului hotărârii de Guvern** **Obiecții:** Potrivit punctului 22 din proiect, autoritatea de aplicare a legii care a utilizat derogarea prevăzută la punctul 21 are obligația de a informa Punctul Unic de Contact și de a transmite copia solicitării imediat ce circumstanțele excepționale care au justificat măsura nu mai există. În materia investigațiilor penale complexe (în special cele privind corupția, criminalitatea organizată sau alte infracțiuni grave) necesitatea menținerii stricte a confidențialității poate persista pe întreaga durată a urmăririi penale sau chiar și în fazele ulterioare ale procesului penal. În absența unor repere clare, responsabilii de executare se vor afla în imposibilitatea de a stabili cu certitudine momentul exact în care obligația de informare devine posibilă și, în consecință, există un risc real ca aceasta să nu fie executată. Totodată, proiectul nu instituie un termen obiectiv, un mecanism procedural clar sau responsabilități clare pentru monitorizarea acestei obligații, ceea ce afectează previzibilitatea normei și face imposibil controlul respectării acesteia. În aceste condiții, menținerea punctului 22 afectează calitatea actului normativ prin nerespectarea exigențelor de certitudine și previzibilitate, creând premise pentru o aplicare neunitară și defectuoasă. **Recomandări:** Recomandăm excluderea punctului 22 din proiect.	**Nu se acceptă** Norma de la pct. 22 reprezintă transpunerea fidelă a Art. 6 din Directiva (UE) 2023/977, care stipulează că derogarea de la informarea PUC este una strict temporară și excepțională. Restabilirea informării este obligatorie pentru a asigura integritatea bazei de date de triaj și funcția de verificare încrucișată (cross-checking), prevenind astfel suprapunerea investigațiilor sau interpelările divergente pe același caz. Deși circumstanțele excepționale nu sunt detaliate cronologic, acestea încetează, de regulă, odată cu trecerea investigației într-o fază publică, moment în care riscul de periclitare a probatoriului dispare. Securitatea informațiilor transmise ulterior este garantată prin jurnalizarea operațiunilor pe o perioadă de 3 ani și monitorizarea de către CNPDCP, asigurând conformitatea administrativă fără riscuri operative suplimentare. În concluzie, eliminarea acestei obligații ar constitui o transpunere defectuoasă a acquis-ului comunitar, riscând

			declanșarea procedurii de constatare a neîndeplinirii obligațiilor (infringement) de către Comisia Europeană și subminând rolul strategic al PUC în coordonarea cooperării polițienești internaționale.
	118	**Obiecție generală la anexa nr.1 potrivit proiectului hotărârii de Guvern** **Obiecții:** Din analiza textului proiectului de act normativ propus, se atestă un vid normativ în cea ce privește reglementarea expresă a procesului de creare, administrare, gestionare a conturilor de utilizator (user accounts) pentru autoritățile de aplicare a legii în sistemele europene de schimb de informații (SIENA, EUCARIS, CIR etc.). Deși, proiectul stabilește că Punctul Unic de Contact utilizează aceste sisteme și că personalul PUC și PNC are acces la acestea, se omite să se reglementeze aspectele procedurale esențiale, precum subiectul responsabil de crearea, validarea și revocarea conturilor de utilizator, procedura și criteriile de aprobare a accesului, stabilirea nivelurilor de acces, mecanismul prin care alte autorități (CNA, SIS etc.) pot solicita și obține utilizatori proprii pentru îndeplinirea competențelor legale. În lipsa unor prevederi clare, există riscul ca administratorul tehnic al sistemului să interpreteze arbitrar procedura de creare a utilizatorilor, iar autoritățile de aplicare a legii cu rol important în prevenirea și combaterea criminalității sau corupției (ex. CNA) să fie private de un acces operativ și securizat la platformele europene. Acest fapt contravine principiului previzibilității actului normativ, creând premise pentru aplicarea unor tratamente diferențiate sau abuzive în raport cu solicitanții de acces. În cazul în care CNA sau alte autorități necesită să utilizeze aceste sisteme în activitatea sa, este necesar ca proiectul să prevadă expres procedura de obținere a utilizatorilor, ca de exemplu: *„Autoritățile de aplicare a legii desemnate potrivit legii pot solicita crearea conturilor de utilizator pentru personalul propriu autorizat, în vederea utilizării sistemelor SIENA, EUCARIS și a altor platforme europene de schimb de informații, în limitele competențelor legale și potrivit regulilor de administrare aprobate de administratorul sistemului.”*	**Nu se acceptă** Conform art. 6 alin. (1) din Legea nr. 209/2026 privind cooperarea polițienească internațională și pct. 4 din Anexa nr.1 a proiectului hotărârii de Guvern, DCPI este desemnat drept punct unic de contact (*Single Point of Contact*), având responsabilitatea exclusivă de coordonare și gestionare centralizată a schimbului internațional. Arhitectura tehnică a proiectului nu prevede accesul direct al altor autorități la platformele europene prin conturi individuale, ci un mecanism de interconectare a sistemelor. Proiectul instituie platforma guvernamentală de interoperabilitate *MConnect* drept canal principal de comunicare pe segmentul național. Această platformă alimentează automatizat interfețele tehnice internaționale (Router UE, EPRIS, EUCARIS), eliminând necesitatea unor conexiuni „punct-la-punct” sau a creării de conturi de utilizator externe pentru personalul PNC. Potrivit pct. 5 și pct. 11 din Anexa nr. 2 a proiectului hotărârii de Guvern, schimbul de date și consumarea acestora de către PNC-uri se realizează prin interogări în sistemele naționale, datele fiind tranzitate securizat prin MConnect către PUC, care asigură interfața cu partenerii externi. Acest model garantează securitatea maximă și trasabilitatea fluxurilor de

		O astfel de completare este importantă deoarece, în forma actuală, reglementarea strict tehnică a platformelor, fără stabilirea unui regim juridic clar al utilizatorilor și al drepturilor de acces, afectează trasabilitatea acțiunilor și controlul intern, elemente fundamentale pentru prevenirea incidentelor de integritate în gestionarea informațiilor restricționate. **Recomandări:** Reconsiderarea prevederilor anexei nr.1 potrivit proiectului conform obiecțiilor expuse supra.	date, fără a multiplica punctele de acces la infrastructura critică a UE (rețeaua TESTA). Desemnarea nominală a persoanelor autorizate în cadrul fiecărui PNC (pct. 34 din Anexa nr. 2 a proiectului hotărârii de Guvern) are scopul de a asigura trasabilitatea acțiunilor în log-urile MConnect și în sistemele naționale, nu de a obține conturi de acces în aplicații administrate de Europol sau eu-LISA. Astfel, solicitarea de a reglementa crearea de conturi de utilizator externe pentru autoritățile de aplicare a legii este neîntemeiată, deoarece participarea acestora la schimbul de date este asigurată prin interoperabilitatea sistemelor naționale (MConnect) sub coordonarea tehnică și operativă a PUC.
Ministerul Justiției (nr. 04/1-7957 din 15.07.2026)	**119**	***La proiectul hotărârii:*** La subpct. 1.2, domeniul atribuit Serviciului Tehnologii Informaționale se va corela cu prevederile art. 20 și 21 din proiectul Legii privind cooperarea polițienească internațională. Or, proiectul hotărârii include în sfera de competență a Serviciului „evidențele poliției cu caracter criminal, contravențional” și datele nominale privind „persoanele urmărite, dispărute fără veste sau implicate în activități infracționale”, în timp ce proiectul legii circumscrie schimbul automatizat prin EPRIS la evidențele poliției referitoare la persoanele reținute, bănuite, învinuite și condamnate, iar accesul la date privind victimele, martorii sau persoanele dispărute fără veste este admis doar în cazurile speciale prevăzute expres de lege.	**Se acceptă** Proiect ajustat, prin: - modificarea subpct. 1.2. din partea dispozitivă a proiectului hotărârii de Guvern; - modificarea supct. 4.2. din Anexa nr. 2 a proiectului hotărârii de Guvern.
	120	***La regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații:*** Cu referire la denumirea Regulamentului din anexa nr. 1, aceasta se va corela cu denumirea indicată la subpct. 2.1 din proiectul hotărârii și se va expune după următoarea formulă: „Regulamentul privind organizarea și funcționarea Punctului Unic de Contact în scopul schimbului de date și informații”. Observația dată este valabilă, în mod corespunzător, și pentru	**Se acceptă** Proiect ajustat prin: - modificarea denumirii anexelor nr. 1 și nr. 2 a proiectului hotărârii de Guvern.

		denumirea Regulamentului din anexa nr. 2, prin raportare la subpct. 2.2 din proiectul hotărârii.	
	121	La pct. 1, enumerarea categoriilor de date care fac obiectul schimbului de date și informații se va corela cu art. 2 alin. (2) și (4) din proiectul Legii privind cooperarea polițienească internațională. Or, potrivit art. 2 alin. (2) din proiectul legii, datele furnizate în scopul interogării directe sau automatizate a bazelor de date se limitează strict la categoriile prevăzute expres în lege, iar alin. (4) al aceluiași articol stabilește categoriile de date care pot face obiectul schimbului informațional internațional, inclusiv automatizat.	**Se acceptă** Proiect ajustat prin: - modificarea pct. 1 din Anexa nr. 1 a proiectului hotărârii de Guvern.
	122	La pct. 4, cuvintele „Single Point of Contact” se vor exclude. Or, în proiectul legii privind cooperarea polițienească internațională, structura respectivă este desemnată prin noțiunea „Punctul Unic de Contact” și abrevierea „PUC”, motiv pentru care utilizarea concomitentă a denumirii în limba engleză poate genera paralelism terminologic.	**Se acceptă** Proiect ajustat prin: - modificarea pct. 4 din Anexa nr. 1 a proiectului hotărârii de Guvern.
	123	În mod corespunzător, subpct. 5.12 se va exclude ca fiind redundant, întrucât definește aceeași structură instituțională reglementată deja prin noțiunea „Punctul Unic de Contact”.	**Se acceptă** Proiect ajustat prin: - excluderea subpct. 5.12. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	124	Se recomandă revizuirea terminologiei utilizate la subpct. 5.2–5.6, 5.13 și 5.14 din proiect, prin asigurarea conformității acesteia cu exigențele de tehnică legislativă prevăzute de *Legea nr. 100/2017 cu privire la actele normative*. Astfel, proiectul utilizează o serie de denumiri în limba engleză (Common Identity Repository – CIR, Common Repository for Reporting and Statistics – CRRS, European Search Portal – ESP, European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice – eu-LISA), fără a indica în mod clar corespondentul terminologic în limba română. În conformitate cu principiile de elaborare a proiectelor actelor normative, utilizarea termenilor din alte limbi este admisibilă atunci când este necesară, însă aceștia urmează a fi redați prin indicarea echivalentului sau explicației în limba română. În acest sens, se recomandă ca la prima utilizare a fiecărui termen să fie indicată denumirea în limba română, urmată, după caz, de denumirea oficială în limba engleză și abrevierea consacrată.	**Se acceptă** Proiect ajustat prin: - modificarea subpct. 5.2.-5.6., 5.13. și 5.14. din Anexa nr. 1 a proiectului hotărârii de Guvern.

	125	La subpct. 11.1, norma privind notificarea oficială se va corela cu art. 53 alin. (7) din proiectul Legii privind cooperarea polițienească internațională. Potrivit normei legale menționate supra, Punctul Unic de Contact notifică oficial Comisia Europeană, Agenția eu-LISA și Europol cu privire la identitatea și datele de legătură ale punctelor naționale de contact desemnate conform art. 6 din lege. În acest sens, se va examina oportunitatea excluderii referinței la Secretariatul General al Consiliului Uniunii Europene.	**Se acceptă** Legea nr. 209/2026 privind cooperarea polițienească internațională va fi ajustat, pentru a asigura o corelare tehnică și juridică perfectă între prevederile art. 53 alin. (7) din proiectul de Lege și atribuțiile PUC stabilite în proiectul hotărârii de Guvern.
	126	La pct. 25 și 26, dispozițiile privind derogarea de la termenele maxime de furnizare a informațiilor se vor corela. Or, pct. 25 exclude posibilitatea prelungirii termenelor prin invocarea volumului datelor sau a complexității verificărilor, dacă acestea nu constituie motive obiective de imposibilitate a furnizării, în timp ce pct. 26 admite nerespectarea termenelor „din cauza complexității cererii”. În vederea evitării unor interpretări contradictorii, textul se va reformula prin stabilirea unitară și exhaustivă a cazurilor în care este permisă derogarea de la termenele prevăzute la pct. 24.	**Se acceptă** Proiect ajustat prin: - modificarea pct. 26 din Anexa nr. 1 a proiectului hotărârii de Guvern.
	127	La pct. 53, se va utiliza noțiunea „infracțiunilor cu caracter terorist”, în acord cu prevederile art. 134^{11} din *Codul penal* nr. 985/2002. Observația dată este valabilă pentru toate cazurile similare din proiect (pct. 75, 76 și 78 din anexa nr. 2).	**Se acceptă** Proiect ajustat prin: - modificarea pct. 53 din Anexa nr. 1 a proiectului hotărârii de Guvern.
	128	La pct. 75, cuvintele „pentru menținerea siguranței publice” se vor substitui cu cuvintele „în scopul prevenirii, depistării și investigării infracțiunilor”, în vederea corelării cu art. 15 din proiectul Legii privind cooperarea polițienească internațională.	**Se acceptă** Proiect ajustat prin: - modificarea pct. 75 din Anexa nr. 1 a proiectului hotărârii de Guvern.
	129	La pct. 94, se va revedea trimiterea la art. 40 din proiectul legii privind cooperarea polițienească internațională, întrucât norma menționată din proiectul legii reglementează utilizarea armamentului, munițiilor și echipamentelor, și nu regimul păstrării înregistrărilor/log-urilor, motiv pentru care se va rectifica.	**Se acceptă** Proiect ajustat prin: - modificarea pct. 94 din Anexa nr. 1 a proiectului hotărârii de Guvern.
	130	***La Regulamentul de organizare și funcționare a Punctelor Naționale de Contact în scopul schimbului de date și informații***: La pct. 10, cuvintele „și corecta” se vor exclude, în vederea evitării dublării acestora.	**Se acceptă** Proiect ajustat prin: - modificarea pct. 10 din Anexa nr. 2 a proiectului hotărârii de Guvern.
	131	Se recomandă revizuirea pct. 40, întrucât formularea „încălcarea dispozițiilor prezentului Regulament” nu asigură suficientă claritate și	**Se acceptă** Proiect ajustat, prin:

		previzibilitate normei. Trimiterea generală la încălcarea „dispozițiilor prezentului Regulament” nu permite identificarea concretă a conduitei ilicite, a obligațiilor încălcate sau a normelor a căror nerespectare ar putea constitui temei pentru angajarea unei anumite forme de răspundere juridică. Adițional, se va ține cont că, prevederile generale privind survenirea răspunderii pentru nerespectarea dispozițiilor normative poartă un caracter declarativ, or, răspunderea juridică trebuie să fie prevăzută de normele materiale, ce stabilesc tipul concret de răspundere (civilă, contravențională sau penală), determină faptele și sancțiunile pentru comiterea acestora.	- modificarea pct. 109. din Anexa nr. 1 a proiectului hotărârii de Guvern; - modificarea pct. 40. din Anexa nr. 2 a proiectului hotărârii de Guvern.
	132	La pct. 75, atribuțiile Serviciului de Informații și Securitate se vor corela cu obiectul desemnării prevăzut la subpct. 1.5 din proiectul hotărârii. Observația dată este valabilă și pentru pct. 79.	**Se acceptă** Proiect ajustat, prin: - modificarea pct. 75. și 79. din Anexa nr. 2 a proiectului hotărârii de Guvern.
DCPI a IGP (nr. 34/10 – 13890 din 10.07.2026)	**133**	Se propune completarea pct. 1 din proiect cu desemnarea suplimentară a unor autorități în calitate de Puncte Naționale de Contact, și anume: Inspectoratul General al Poliției de Frontieră – pe domeniul controlului și supravegherii frontierei de stat și al informațiilor aferente criminalității transfrontaliere; Centrul Național Anticorupție – având în vedere solicitarea autorității de a fi inclusă în arhitectura instituțională a schimbului de date și informații, precum și competența sa funcțională în domeniul prevenirii și combaterii corupției, investigării infracțiunilor conexe și recuperării bunurilor infracționale; Inspectoratul General al Poliției, prin Inspectoratul Național de Investigații – pentru domeniul investigativ-operativ, și prin Inspectoratul Național de Securitate Publică – pentru domeniul ordinii și securității publice. Propunerea este determinată de necesitatea corelării listei PNC cu competențele funcționale ale autorităților naționale care deține, utilizează sau furnizează date și informații relevante pentru cooperarea polițienească internațională, precum și de asigurarea unei delimitări instituționale mai clare a domeniilor de responsabilitate în cadrul mecanismului național instituit prin proiect.	**Nu se acceptă** A se vedea obiecția cu nr. 114.
	134	Completarea pct. 5 subpct. 11, în partea textului inserat în paranteză, cu autoritățile propuse spre includere la pct. 1 din proiect, și anume: CNA , IGPF, INI, INSP, în vederea corelării dispozițiilor proiectului și a reflectării corespunzătoare a competențelor instituționale relevante.	**Se acceptă** Proiect ajustat prin: - modificarea subpct. 5.11. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	135	Înlocuirea definiției actuale de la pct. 5.12 cu definiția de mai jos, întrucât aceasta reflectă mai fidel rolul Punctului Unic de Contact în arhitectura națională de cooperare polițienească internațională, aliniind	**Se acceptă parțial** Noțiunea a fost exclusă, a se vedea obiecțiile cu nr. 122 și 123.

		terminologia la standardele utilizate în actele Uniunii Europene și în tratatele internaționale la care Republica Moldova este parte: *Single Point of Contact (SPOC) – structură administrativă și operațională desemnată la nivel național ca punct unic de contact pentru schimbul de informații între autoritățile de aplicare a legii ale statului și cele ale altor state membre ale Uniunii Europene, state terțe, precum și cu organizațiile internaționale în domeniul aplicării legii, prin utilizarea canalelor de comunicare securizate stabilite de legislația Uniunii Europene și de tratatele internaționale la care Republica Moldova este parte*.	
	136	Modificarea locului Secțiunii 1 „Principiile de activitate ale PUC”, astfel încât aceasta să fie inclusă în introducerea comună pentru Punctul Unic de Contact și Punctele Naționale de Contact, deoarece principiile nu privesc doar activitatea PUC, ci se aplică tuturor autorităților implicate în schimbul de date și informații, acestea fiind principii-cadru aplicabile oricărei activități polițienești și de cooperare.	**Se acceptă** Proiect ajustat prin: - modificarea pct. 7. din Anexa nr. 2 a proiectului hotărârii de Guvern.
	137	La pct. 10 subpct. 1, se propune modificarea textului, după cum urmează: „*Secția Europol asigură, la nivel național, schimbul de date și informații prin intermediul Router-ului Prüm II și al sistemului EPRIS, în calitate de structură desemnată pentru coordonarea operațională, transmiterea și recepționarea solicitărilor, în condițiile competențelor prevăzute de cadrul normativ aplicabil*”. Modificarea este necesară pentru a clarifica faptul că Secția Europol are rolul de coordonare și asigurare operațională a schimbului de date la nivel național, fără ca acestei structuri să-i fie atribuită responsabilitatea pentru administrarea tehnică a infrastructurii centrale a Uniunii Europene, respectiv Router-ul Prüm II și sistemul EPRIS, care ține de competența structurilor europene abilitate.	**Se acceptă** Proiect ajustat prin: - modificarea subpct. 10.1. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	138	Se propune completarea pct. 10 subpct. 4, după cum urmează: „*Secția cooperare polițienească – coordonează schimbul de date și informații în contextul evenimentelor cu dimensiune transfrontalieră, inclusiv al celor majore*.”	**Nu se acceptă** Legea nr. 209/2026 privind cooperarea polițienească internațională consacră și definește la Articolul 3 alineatul (2) punctul 16 o singură categorie juridică specifică: „eveniment major cu dimensiune transfrontalieră”. Această noțiune include evenimente de amploare (competiții sportive, summituri, conferințe internaționale) care, prin importanța lor, pot genera riscuri la

			adresa ordinii publice și necesită cooperare internațională.
	139	Modificarea pct. 11 subpct. 4, prin excluderea cuvântului „*operativă*” din formularea actuală.	**Se acceptă** Proiect ajustat prin: - modificarea subpct. 11.4. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	140	Revizuirea pct. 11 subpct. 5, prin separarea clară a referințelor la sistemul EPRIS de cele privind datele dactiloscopice, cu reformularea normei după cum urmează: „*realizarea schimbului de date și informații prin sistemul EPRIS, utilizând instrumentul de căutare pentru interogarea registrelor naționale de evidențe ale poliției, inclusiv a datelor de evidență privind persoanele urmărite, dispărute fără veste sau implicate în activități infracționale, pe baza indicilor de evidență polițienească*.”. Totodată, pentru componenta dactiloscopică se propune utilizarea unei formulări distincte și editarea unui nou subpunct, după cum urmează: „*realizarea schimbului de date dactiloscopice se face prin intermediul Router-ului Prüm II, pe baza interogărilor automatizate ale bazelor de date naționale de dactiloscopie, în cooperare cu Punctul Național de Contact competent și cu respectarea condițiilor și procedurilor prevăzute de Regulamentul (UE) 2024/982*”. Sistemul EPRIS este destinat interogării indicilor evidențelor polițienești, în timp ce datele dactiloscopice fac parte din componenta biometrică a schimbului automatizat realizat prin Router-ul Prüm II.	**Se acceptă** Proiect ajustat prin: - modificarea subpct. 11.5. din Anexa nr. 1 a proiectului hotărârii de Guvern; - includerea noului subpct. 11.6. în Anexa nr. 1 a proiectului hotărârii de Guvern.
	141	Se propune revizuirea pct. 11 subpct. 9, și reformularea textului după cum urmează: „*gestionarea, la nivel de coordonare și schimb de informații, a procedurilor de dare în urmărire internațională, de localizare a persoanelor dispărute fără veste în contextul cauzelor penale sau din motive umanitare, de identificare a cadavrelor ori a părților precum și a procedurilor de predare și preluare a persoanelor urmărite sau căutate, desfășurate prin canalele de cooperare polițienească internațională, în condițiile competențelor prevăzute de cadrul normativ aplicabil*”. Astfel, se clarifică faptul că PUC/SPOC doar coordonează și gestionează schimbul de informații în aceste proceduri (urmărire internațională, persoane dispărute, cadavre, predare/preluare), iar deciziile juridice țin de autoritățile competente.	**Se acceptă** Proiect ajustat prin: - modificarea subpct. 11.10. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	142	La pct. 11 subpct. 10, se propune reformularea textului, astfel ca după sintagma „infracțiunile transfrontaliere” să se regăsească textul „*inclusiv traficul ilicit de vehicule și alte forme de criminalitate organizată*	**Se acceptă** Proiect ajustat prin:

		relevante", pentru a nu limita domeniul de cooperare cu Europol și accesul la bazele de date.	- modificarea subpct. 11.11. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	143	La pct. 11 subpct. 11, se propune reformularea textului după cum urmează: „*asigurarea suportului informațional și de coordonare pentru operațiuni comune, supravegheri și urmăriri transfrontaliere, desfășurate prin canalele de cooperare polițienească internațională, în colaborare cu autoritățile competente*". Partea a doua a punctului se dublează în conținutul pct. 11.9.	**Se acceptă** Proiect ajustat prin: - modificarea subpct. 11.12. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	144	La pct. 16, se propune completarea cu sintagmele „*asigurând trasabilitatea acțiunilor și termenelor de prelucrare a cererilor de informație și a răspunsurilor și* …(conform textului)".	**Se acceptă** Proiect ajustat prin: - modificarea pct. 16. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	145	Se propune reformularea pct. 24 prin completarea regimului termenelor de răspuns, astfel încât acesta să reflecte nu doar termenele aplicabile schimburilor efectuate prin SIENA, ci și a solicitărilor recepționate prin canalele INTERPOL, având în vedere că PUC/SPOC gestionează, potrivit proiectului, și schimburi operaționale realizate prin Biroul Național Central Interpol și prin canale alternative de cooperare internațională. În acest sens, se consideră oportună includerea, pe lângă termenele prevăzute pentru schimburile realizate prin SIENA, și a următoarelor categorii operaționale utilizate în practica INTERPOL: Flash – cât de curând posibil, imediat, dar nu mai mult de 8 ore; Very urgent – 24 ore; Urgent – 7 zile; Routine – 30 zile. Se recomandă, în special, includerea expresă a termenului aferent categoriei „Routine – 30 zile". O asemenea completare ar permite stabilirea termenelor în funcție de canalul de cooperare utilizat, gradul de urgență și complexitatea solicitării, prevenind întârzierile generate de aplicarea strictă a termenelor restrânși.	**Nu se acceptă** Propunerea este incompatibilă cu Directiva (UE) 2023/977 (transpusă la pct. 3 din PHG), care stabilește un plafon maxim de 7 zile pentru cererile neurgente. Introducerea unui termen de 30 de zile ar submina eficiența Punctului Unic de Contact (PUC) și ar crea un regim dual de raportare, contrar principiului interoperabilității. Mai mult, proiectul interzice expres prelungirea termenelor invocând „complexitatea verificărilor". Punctul Unic de Contact (PUC) are rolul de a centraliza fluxurile, iar aplicația SIENA este canalul prioritar pentru statele membre UE. Deși INTERPOL este utilizat pentru state terțe, PUC trebuie să asigure un standard minim de celeritate (7 zile) pentru a nu periclita investigațiile transfrontaliere și pentru a permite monitorizarea automată în Sistemul electronic de gestionare a cazurilor.
	146	La pct. 78 se impune clarificarea rolului „membrului calificat al personalului", întrucât redactarea actuală poate crea impresia că PUC sau	**Se acceptă** Proiect ajustat prin:

		alte autorități decât CTCEJ efectuează validarea concordanțelor biometrice. Se recomandă precizarea expresă că verificarea manuală a concordanțelor (hits) este realizată exclusiv de un expert criminalist sau alt membru al personalului specializat din cadrul CTCEJ, desemnat prin act administrativ intern, iar PUC are doar rolul de a facilita transmiterea ulterioară a datelor validate.	- modificarea pct. 78. din Anexa nr. 1 a proiectului hotărârii de Guvern.
STI al IGP (nr. 8/5 – 5888 din 10.07.2026)	**147**	Se constată că proiectul utilizează un număr considerabil de abrevieri care nu sunt definite în cuprinsul Regulamentului. În vederea respectării principiilor clarității și previzibilității normelor juridice, se recomandă completarea pct. 5 din Anexa nr. 1 cu definițiile tuturor abrevierilor utilizate în textul proiectului.	**Nu se acceptă** Abrevierile utilizate pe parcursul proiectului hotărârii de Guvern care nu se regăsesc la pct. 5 din Anexa nr. 1, se regăsesc în actul normativ de rang superior și anume Legea nr. 209/2026 privind cooperarea polițienească internațională. Întrucât proiectul hotărârii Guvernului constituie un act normativ subsecvent, elaborat în vederea implementării legii menționate, reiterarea tuturor definițiilor și abrevierilor prevăzute de actul normativ primar ar genera dublări normative nejustificate. Prin urmare, la pct. 5 din Anexa nr. 1 sunt definite doar noțiunile și abrevierile specifice obiectului de reglementare al proiectului hotărârii Guvernului.
	148	Redacția propusă , in special pentru pct. 11 și Secțiunea 1 din Capitolul III din Anexa nr. 1, precum și alte referințe care vizează „Router”, necesită revizuire din perspectiva terminologiei tehnice și a cadrului normativ aplicabil. Sintagma potrivit căreia Punctul Unic de Contact asigură schimbul de informații „prin utilizarea Router-ului și a celorlalte instrumente tehnice de interoperabilitate” nu reflectă în mod corespunzător modul de realizare a schimbului de date cu infrastructurile Uniunii Europene. Comunicarea cu majoritatea resurselor informaționale europene se realizează prin rețeaua TESTA (Trans European Services for Telematics between Administrations), care, potrivit Hotărârii Guvernului nr. 65/2026, este administrată la nivel național de Instituția Publică Serviciul Tehnologia	**Se acceptă** Proiect ajustat prin: - includerea noii noțiuni „ *infrastructură de comunicații securizată* ” la pct. 5. în Anexa nr. 1 a proiectului hotărârii de Guvern; - modificarea pct. 11. din Anexa nr. 1 a proiectului hotărârii de Guvern.

		Informației și Securitate Cibernetică, în calitate de punct național de conectare (Local Domain Connection Point). În acest scop este utilizată o infrastructură securizată alcătuită din mai multe componente tehnice, iar funcționarea acesteia nu se reduce la utilizarea unui singur echipament de tip router, ci presupune utilizarea unui ansamblu de componente și servicii de comunicații. Totodată, noțiunea de interoperabilitate este definită de Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate ca reprezentând capacitatea tehnică a sistemelor informaționale și capacitatea organizatorică a participanților de a reutiliza date printr-un proces eficient de schimb de date. Prin urmare, interoperabilitatea presupune atât componente tehnice, cât și elemente juridice și organizaționale, motiv pentru care nu poate fi redusă la utilizarea unor instrumente tehnice. În acest context, se propune reformularea pct. 11 și înlocuirea, după caz, și Secțiunea 1 din Capitolul III, dar și în conținutul proiectului, care prezumă utilizarea unor noțiuni generale privind infrastructura de comunicații și mecanismele de interoperabilitate, în concordanță cu cadrul normativ național și european, în special înlocuirea noțiunii „Router” prin sintagma „infrastructura/echipamentele de comunicații”.	
	149	Potrivit pct. 16, toate operațiunile de acces și schimb de date urmează să fie înregistrate în Sistemul electronic unic de gestionare a cazurilor. Sub acest aspect, se constată că sistemul informațional menționat nu dispune, la momentul actual, de cadrul juridic necesar funcționării, respectiv de Concepția și Regulamentul aprobate prin hotărâre de Guvern, astfel cum prevăd Legea nr. 467/2003 privind informatizarea și resursele informaționale de stat și Hotărârea Guvernului nr. 562/2006 privind crearea sistemelor și resurselor informaționale automatizate de stat. În consecință, referirea la un sistem informațional care nu este instituit în condițiile legislației în vigoare poate genera obiecții în procesul de avizare, inclusiv din partea Agenției de Guvernare Electronică, autoritatea competentă în domeniul schimbului de date și interoperabilității. Totodată, se recomandă completarea proiectului cu prevederi referitoare la utilizarea resurselor informaționale specializate, inclusiv N.SIS, care realizează schimbul automatizat de date fără intervenția operatorului uman, aspect insuficient reglementat în redactarea actuală.	**Se acceptă parțial** La Legea nr. 209/2026 privind cooperarea polițienească internațională, art 56. - Guvernul în termen de 12 luni, va aproba actul normativ privind aprobarea Concepției și Regulamentului Sistemului electronic unic de gestionare a cazurilor”. Astfel instituirea juridică a Sistemului electronic unic de gestionare a cazurilor (aprobarea Concepției și a Regulamentului acestuia) se va realiza printr-o Hotărâre de Guvern separată, în conformitate cu prevederile Legii nr. 467/2003. Prezentul proiect de Hotărâre reglementează deja rolul funcțional și operativ al acestui sistem în arhitectura Punctului Unic de Contact.

		Aceeași abordare se atestă și pentru prevederile referitoare la componenta națională de interacțiune cu sistemul EPRIS, instituit la nivelul UE.	În conformitate cu clauza de aplicare eșalonată prevăzută la pct. 5 din PHG și Articolul 56 din Proiectul de Lege, interfața cu N.SIS/EPRIS va fi integrată în fluxul de lucru al Sistemului electronic unic de gestionare a cazurilor ulterior obținerii dreptului de acces sau de la data aderării Republicii Moldova la Uniunea Europeană. Se reiterează faptul că N.SIS va fi instituit după obținerea de către Republica Moldova a dreptului de acces la mecanismele respective la data aderării la Uniunea Europeană
	150	Se recomandă revizuirea prevederilor Secțiunii 1 din Anexa nr. 1, din perspectiva securității și confidențialității sistemelor informaționale și de comunicații, prin utilizarea unor formulări cu caracter general referitoare la infrastructura utilizată, care să descrie capacitățile funcționale ale acesteia, fără enumerarea expresă a componentelor tehnice. Totodată, se constată că proiectul nu reglementează în mod suficient arhitectura tehnică și operațională a schimbului de date cu structurile Uniunii Europene, iar unele aspecte sunt tratate fragmentar. În special, se recomandă reglementarea expresă a drepturilor, atribuțiilor și competențelor tuturor autorităților naționale implicate în cooperarea internațională pentru realizarea consultărilor și schimbului de date în domeniul ordinii și securității publice, precum și delimitarea explicită atribuțiilor acestora.	**Se acceptă parțial** Norma prevăzută la pct. 45 din Anexa nr. 1 reprezintă o transpunere obligatorie a Art. 35 alin. (2) din Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024 privind căutarea și schimbul automatizat de date în scopul cooperării polițienești (Regulamentul Prüm II). Proiect ajustat prin: - modificarea pct. 44-46. din Anexa nr. 1 a proiectului hotărârii de Guvern.
	151	Cu privire la prevederile Secțiunii 2 din Capitolul III și ale Secțiunii 2 din Capitolul III al Anexei nr. 2, se exprimă rezerve privind capacitatea legală Serviciului Tehnologii Informaționale de a acorda acces și de a administra sistemul EPRIS. În forma actuală, proiectul nu stabilește mecanismul juridic și tehnic prin care aceste atribuții vor fi exercitate și nici nu reglementează existența componentei naționale care să asigure interoperabilitatea cu sistemul european și evidența auditului accesărilor. Se recomandă instituirea și reglementarea acestei componente în conformitate cu legislația națională privind sistemele informaționale de stat și interoperabilitatea.	**Se acceptă** La Legea nr. 209/2026 privind cooperarea polițienească internațională, art. 56: „*Guvernul în termen de 12 luni, va aproba actul normativ privind aprobarea Concepției și Regulamentului componentei naționale a sistemului EPRIS*”, în vederea instituirii acestuia ca sistem informațional de stat și asigurării deplinei capacități juridice conform Legii nr. 467/2003.

			Proiect ajustat prin: - includerea noului pct. 48 în Anexa nr. 1 a proiectului hotărârii de Guvern.
	152	Cu privire la pct. 4.2 din Anexa nr. 2 - denumirea și atribuțiile Serviciului Tehnologii Informaționale urmează a fi corelate cu prevederile Hotărârii Guvernului nr. 317/2020. Totodată, Vă atenționam că atribuțiile prevăzute în proiect necesită reformulare, întrucât STI nu exercită competențe în domeniul evidențelor polițienești, dar deține calitatea de deținător și administrator al sistemelor informaționale de stat utilizate în acest domeniu, inclusiv Registrul informației criminalistice și criminologice, Registrul de stat dactiloscopic, Sistemul informațional automatizat de evidență a contravențiilor și alte sisteme informaționale specializate. În același context, se recomandă revizuirea prevederilor Capitolului VIII din Anexa nr. 2, astfel încât atribuțiile STI să fie corelate cu competențele stabilite prin actele normative care reglementează sistemele informaționale respective. De asemenea, întrucât competențele STI în raport cu sistemul EPRIS nu sunt reglementate în prezent, este necesară elaborarea și aprobarea cadrului normativ aferent componentei naționale EPRIS sau, după caz, modificarea cadrului normativ aplicabil sistemelor informaționale care vor asigura interoperabilitatea cu acesta. În consecință, se solicită revizuirea de principiu a prevederilor respective.	**Se acceptă** La Legea nr. 209/2026 privind cooperarea polițienească internațională, art. 56: „Guvernul în termen de 12 luni, va aproba actul normativ privind aprobarea Concepției și Regulamentului componentei naționale a sistemului EPRIS”, în vederea instituirii acestuia ca sistem informațional de stat și asigurării deplinei capacități juridice conform Legii nr. 467/2003. Proiect ajustat prin: - modificarea pct. 4.2. din Anexa nr. 1 a proiectului hotărârii de Guvern; - modificarea pct. 48 din Anexa nr. 2 a proiectului hotărârii de Guvern.
	153	Cu privire la pct. 5 din Anexa nr. 2 - prevederea potrivit căreia PNC au obligația de a asigura interoperabilitatea sistemelor proprii cu infrastructura națională prin utilizarea platformei guvernamentale de interoperabilitate MConnect necesită completare. Se recomandă identificarea expresă a resursei informaționale administrate de Punctul Unic de Contact pentru care urmează să fie asigurată interoperabilitatea prin intermediul platformei guvernamentale de interoperabilitate MConnect. Totodată, având în vedere că autoritățile terțe nu dețin competențe de administrare a sistemelor informaționale gestionate de PUC, obligația dezvoltării și punerii la dispoziție a interfețelor de interoperabilitate	**Se acceptă** Proiect ajustat prin: - modificarea pct. 5 din Anexa nr. 2 a proiectului hotărârii de Guvern. Se reține necesitatea clarificării responsabilităților participanților la schimbul de date prin intermediul platformei MConnect. Deși proiectul de lege (Art. 8) și regulamentul PUC (pct. 37, Anexa nr. 1) stabilesc fundamentul juridic pentru Sistemul electronic unic de gestionare a

		necesare schimbului și consumului de date urmează să revină administratorului PUC.	cazurilor, se acceptă ideea că detalierea regimului tehnic și administrativ al acestei resurse informaționale va fi realizată ulterior, prin acte normative de instituire dedicate În acest sens, responsabilitățile tehnice sunt partajate conform rolurilor stabilite în prezentul pachet normativ: Punctele Naționale de Contact (PNC) au obligația de a asigura disponibilitatea și furnizarea datelor de referință din sistemele proprii către nodul central. Punctul Unic de Contact (PUC) asigură recepționarea, triajul și gestionarea operativă a acestor date în scopul cooperării internaționale. Parametrii tehnici specifici, protocoalele de securitate și fluxurile de schimb vor fi definitivate în procesul de interconectare la platforma guvernamentale de interoperabilitate (MConnect), sub coordonarea Agenției de Guvernare Electronică și în conformitate cu standardul UMF, asigurând astfel o implementare eșalonată și adaptată nevoilor operative reale.
	154	Cu privire la pct. 6 din Anexa nr. 2., care să referă la desemnarea subdiviziunilor și persoanelor responsabile din cadrul Punctelor Naționale de Contact, se recomandă completarea notei de argumentare privind impactul instituțional și realizarea unei analize de e impact, prin prisma faptului că reieșind termenul de răspuns prevăzut la pct. 24.1 din proiect (8	**Nu se acceptă** Termenul de 8 ore prevăzut la pct. 24.1 din Anexa nr. 1 este aplicabil Punctului Unic de Contact pentru soluționarea cererilor urgente referitoare la informații direct

		ore pentru cererile urgente privind informațiile direct accesibile), se implică asigurarea continuității activității în regim permanent (24/7). Se menționează că, în prezent, Serviciul Tehnologii Informaționale își desfășoară activitatea în regim obișnuit de lucru (08:00-17:00, luni-vineri), iar intervențiile în afara programului sunt realizate doar la necesitate și nu au caracter permanent. Urmare, în vederea asigurării prevederilor cadrului normativ de referință promovat prin proiect, se impune instituirea unor subdiviziuni ori funcții de personal specializate cu program de activitate 24/7.	accesibile și nu instituie obligația fiecărui Punct Național de Contact de a desfășura activitate permanentă în regim 24/7. Informațiile direct accesibile sunt consultate de personalul autorizat al PUC prin intermediul sistemelor și resurselor informaționale disponibile, fără intervenția personalului PNC la fiecare solicitare. Pct. 6 din Anexa nr. 2 reglementează exclusiv desemnarea subdiviziunilor și a persoanelor responsabile din cadrul PNC și nu impune instituirea unor subdiviziuni noi, suplimentarea statelor de personal sau organizarea obligatorie a activității în schimburi permanente. Modalitatea de asigurare a disponibilității sistemelor și de intervenție în cazul incidentelor tehnice ține de organizarea internă a fiecărei autorități și poate fi realizată prin mecanisme de permanență, intervenție la necesitate ori monitorizare tehnică automatizată. Întrucât proiectul nu instituie obligația creării unor funcții sau subdiviziuni specializate cu program 24/7, completarea notei de fundamentare cu un impact instituțional și financiar în acest sens nu este justificată.
Inspectoratul General de Carabinieri	**155**	... și reieșind din atribuțiile statuate conform cadrului normativ, comunică susținerea acestuia, fără obiecții sau propuneri de modificare.	**S-a luat act**

(nr. 1/4 – 1291 din 06.07.2026)			
Procuratura Generală (mențiune pe e-Legiferare)	**156**	Obiecții, comentarii sau propuneri suplimentare nu sunt.	**S-a luat act**
Centrul de Armonizare a Legislației (mențiune pe e-Legiferare)	**157**	CAL validează PHG în lipsa unor observații suplimentare.	**S-a luat act**
Ministerul Finanțelor (mențiune pe e-Legiferare)	**158**	Proiectul de hotărâre a fost prezentat către MF spre informare, iar obiecțiile exprimate anterior au fost luate în considerare.	**S-a luat act**
Centrul Național pentru Protecția datelor cu Caracter Personal (mențiune pe e-Legiferare)	**159**	Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova a examinat repetat *proiectul de hotărâre cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații* (**număr unic 519/MAI/2026**), autor – Ministerul Afacerilor Interne și, în limitele competenței sale, comunică despre lipsa propunerilor și obiecțiilor pe marginea acestuia.	**S-a luat act**
Consiliul Superior al Magistraturii (mențiune pe e-Legiferare)	**160**	CSM comunică lipsa obiecțiilor și propunerilor suplimentare.	**S-a luat act**
EXPERTIZA DE COMPATIBILITATE COMISIA EUROPEANĂ			
Comisia Europeană Raportul recepționat la 28.09.2026	**161**	*Clauza enumeră Poziția comună 2005/69/JAI a Consiliului, dar nu a fost prezentat niciun tabel de concordanță pentru actul respectiv. În plus, în expunerea de motive se afirmă că proiectul de decizie asigură transpunerea parțială a actelor UE enumerate, în timp ce nota din aceeași secțiune prevede că proiectul de lege și proiectul de decizie asigură împreună transpunerea integrală a acestora. Constatările prezentului raport vin în sprijinul primei declarații.* **Recomandare** Să prezinte un tabel de concordanță pentru Poziția comună 2005/69/JAI a Consiliului sau să o elimine din clauza de armonizare în cazul în care este transpusă printr-un alt act. Alinierea notei din expunerea de motive la declarația potrivit căreia transpunerea este parțială.	**Se acceptă** Poziția comună 2005/69/JAI a Consiliului a fost exclusă din clauza de armonizare a *Proiectului de Hotărâre a Guvernului cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații*.
	162	**Punctul 1** desemnează cinci puncte naționale de contact: centrul Tehnic Criminalistic și Expertiză Judiciară din cadrul Inspectoratului General al Poliției (profiluri ADN, date dactiloscopice și imagini faciale); serviciul Tehnologiile Informației (evidențe ale poliției, date nominale, vehicule	**Se acceptă** Prima parte a recomandării ține de aspectele legate de traducerea eronată.

		căutate și Registrul dactiloscopic de stat); Inspectoratul General al Carabinierilor (evenimente majore cu o dimensiune transfrontalieră); Agenția pentru servicii publice (vehicule, documente de identitate și permise de conducere); și Serviciul de Informații și Securitate (informații pentru prevenirea infracțiunilor de terorism). *Aliniere deplină. Desemnările pun în aplicare articolul 30 din Regulamentul Prüm II, articolele 15 și 16 alineatul (3) din Decizia 2008/615/JAI a Consiliului și articolul 5 alineatul (1) din Decizia 2004/919/CE a Consiliului. Cu toate acestea, punctul 1.5 menționează „Serviciul de informații și de securitate”, în timp ce capitolul XI din anexa 2 menționează „Serviciul de securitate și de informații”. Capitolul XII din anexa 2 atribuie sarcini Serviciului de tehnologia informației și securitate cibernetică ca punct local de conectare la rețeaua TESTA, dar serviciul respectiv nu este menționat la punctul 1, iar statutul său nu este precizat*. **Recomandare** Utilizați în mod consecvent denumirea oficială a Serviciului de securitate și informații. Indicați în partea dispozitivă statutul și rolul Serviciului de tehnologie a informației și securitate cibernetică ca punct național de conectare la rețeaua TESTA.	STISC în calitate de punct de conectare a fost inclus în partea dispozitivă a *Proiectului de Hotărâre a Guvernului cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații*.
	163	**Capitolul I** stabilește obiectul, definițiile și cadrul de funcționare ale punctului de contact unic. *Aliniere deplină. Definițiile autorității de aplicare a legii desemnate, informațiile disponibile, informațiile direct accesibile și informațiile indirect accesibile reproduc articolul 2 din Directiva (UE) 2023/977.* *Aliniere parțială. Alineatele (3) și (4), coroborate cu articolul 2 alineatul (3) litera (a) din proiectul de lege, abordează acordurile bilaterale și multilaterale, dar nu reflectă pe deplin domeniul de aplicare și limitele articolului 1 alineatul (2) din Directiva (UE) 2023/977.* *Nealiniată. Alineatele (5.9) și (5.10) definesc tipurile de informații, dar nu reflectă norma prevăzută la articolul 1 alineatul (3) litera (a) din Directiva (UE) 2023/977, conform căreia nu există nicio obligație de a obține informații prin măsuri coercitive.* *Alineatul (1) introduce acronimul „UCP” pentru punctul unic de contact, dar acronimul este utilizat o singură dată. Restul textului utilizează „PUC” (142 ocurențe) și „UPC” (27 ocurențe). Punctele naționale de contact sunt denumite „PNC” (28 de apariții) și „PNC” (18 de apariții).*	**Se acceptă** Limitarea domeniului de aplicare indicate din Directiva 2023/977 au fost incluse în prevederile pct. 2 din Anexa nr. 1 a *Proiectului de Hotărâre a Guvernului cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații*.

		Recomandare Reflectarea în capitolul I a limitării domeniului de aplicare de la articolul 1 alineatul (2) și a normei de la articolul 1 alineatul (3) litera (a) din Directiva (UE) 2023/977. Utilizați un acronim pentru punctul de contact unic și un acronim pentru punctele de contact naționale în ambele anexe și în expunerea de motive.	
	164	**Capitolul VI** reglementează colectarea și furnizarea de statistici, inclusiv raportarea către Comisia Europeană până la data de 1 martie a fiecărui an și indicatorii specifici pentru router, EPRIS și EUCARIS. *Aliniere deplină. Capitolul VI pune în aplicare articolul 18 din Directiva (UE) 2023/977 și articolul 72 alineatul (1)-(3) din Regulamentul Prüm II.* *Nealiniată. Capitolul VI nu reflectă obligațiile prevăzute la articolul 80 alineatul (9), (10) și (11) din Regulamentul Prüm II de a furniza eu-LISA, Comisiei Europene și Europol informațiile necesare pentru rapoartele de evaluare, inclusiv numărul de concordanțe confirmate în fiecare bază de date națională.* **Recomandare** Completarea capitolului VI cu obligațiile prevăzute la articolul 80 alineatul (9), (10) și (11) din Regulamentul Prüm II, sub rezerva aplicării condiționate de la punctul 5.	**Se acceptă** Norma a fost integrată la pct. 132 din Anexa nr. 1 a *Proiectului de Hotărâre a Guvernului cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații*, stabilind obligația de furnizare către Comisia Europeană, eu-LISA și Europol a datelor necesare pentru rapoartele de evaluare (inclusiv numărul concordanțelor confirmate pe categorii/tipuri de date), cu protejarea investigațiilor.
	165	**Capitolele VII-XII** stabilesc sarcinile specifice ale Centrului tehnic criminalistic și ale expertizei judiciare împreună cu Serviciul Tehnologia Informației (date biometrice și validarea concordanțelor), Serviciul Tehnologia Informației (evidențe ale poliției, date dactiloscopice și EPRIS), Inspectoratul General al Carabinierilor (evenimente majore), Agenția pentru Servicii Publice (vehicule, documente și permise de conducere), Serviciul de Securitate și Informații (prevenirea infracțiunilor de terorism) și Serviciul Tehnologia Informației și Securitate Cibernetică (punctul de conexiune TESTA). *Aliniere deplină. Capitolul IX pune în aplicare articolele 13 și 15 din Decizia 2008/615/JAI a Consiliului, inclusiv furnizarea de date fără caracter personal la cerere și din proprie inițiativă. Capitolul X pune în aplicare articolele 5 și 6 din Decizia 2004/919/CE a Consiliului, inclusiv retragerea imediată a semnalărilor. Capitolul XI pune în aplicare articolul 16 din Decizia 2008/615/JAI a Consiliului. Cu toate acestea, titlul*	**Precizare** Recomandarea ține de aspectele legate de traducerea eronată.

		capitolului IX păstrează denumirea în limba română de „Inspectoratul General de Carabinieri”. **Recomandare** Utilizați denumirea în limba engleză a Inspectoratului General al Carabinierilor în titlul capitolului IX.	
	166	**Dispoziții care nu au fost transpuse în niciun act prezentat.** Tabelele de concordanță nu identifică nicio dispoziție națională pentru definițiile termenilor „notă” [articolul 2 litera h) din Decizia 2008/616/JAI a Consiliului] și „candidat” (articolul 4 din Regulamentul Prüm II). Acestea fac referire la transpunerea articolului 27 și a articolului 28 alineatele (1)-(3) din Regulamentul Prüm II în reglementările naționale privind cazierele judiciare, care nu au fost prezentate. *Nealiniată. Explicația potrivit căreia conceptul de „notă” a fost absorbit în confirmarea unei concordanțe în urma unei examinări manuale apare numai în tabelul de corespondență. Termenul „candidat” este utilizat în normele privind capacitățile de căutare fără a fi definit. Numerele de referință și normele privind cererile și răspunsurile pentru evidențele poliției nu au niciun temei obligatoriu în actele prezentate.* **Recomandare** Se introduc definițiile termenilor „notă” și „candidat”. Să stabilească normele privind numerele de referință ale evidențelor poliției și privind cererile și răspunsurile sau să precizeze instrumentul și calendarul adoptării acestora.	**Se acceptă** Noțiunile au fost integrate la pct. 5 din Anexa nr. 1 a *Proiectului de Hotărâre a Guvernului cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații*. Au fost stabilite normele-cadru privind numerele de referință ale evidențelor poliției la pct. 82 din Anexa nr. 1 a proiectului.
	167	**2.2.1. Domeniul de aplicare al evaluării și al prezentării tabelelor de concordanță** În tabelele de concordanță pentru Decizia 2004/919/CE a Consiliului și pentru Regulamentul Prüm II, dispozițiile altor proiecte de hotărâri ale guvernului sunt enumerate în coloana 7, care este destinată actului care face obiectul evaluării. În tabelul de corespondență pentru Regulamentul Prüm II, proiectul de decizie este citat în coloana 7 numai în legătură cu articolele 34-40, 41-45, 46, 48, 51, 53-54 și 59. Celelalte acte ar trebui enumerate în coloana 9. În unele locuri, tabelul conține informații care nu au legătură cu dispozițiile corespunzătoare ale UE. Mai multe trimiteri la alineate nu corespund numerotării din proiectul de decizie: tabelul de concordanță pentru Directiva (UE) 2023/977 citează punctele 31 și 32 din anexa 1 pentru articolul 6 alineatul (3), care sunt punctele 34 și 35 din proiectul de decizie,	**Precizare** Conform Raportului de evaluare (pct. 2.2.1), observațiile au caracter pur tehnico-redacțional („chestiuni de rearanjarea conținutului între coloanele 7 și 9 și actualizarea numerotării”) și nu reprezintă deficiențe de transpunere. Tabelele de concordanță au fost modificate conform recomandării.

		și punctul 114 pentru articolul 16 alineatul (4), care este punctul 116. Tabelul de concordanță pentru Decizia 2008/615/JAI a Consiliului citează alineatele (29) și (30) din anexa 2 pentru articolul 28 alineatul (2), care sunt alineatele (30) și (31). În același tabel, coloana 6 citează articolul 21 alineatul (5) ca referindu-se la „abatere gravă sau abatere săvârșită cu intenție”, în timp ce textul oficial în limba engleză se referă la neglijență gravă sau abatere săvârșită cu intenție. Coloana 10 descrie articolul 41 alineatul (5) din proiectul de lege ca referindu-se numai la comportamentul intenționat, în timp ce textul citat în coloana 9 acoperă, de asemenea, neglijența gravă. Articolele care nu sunt enumerate în tabelele de corespondență nu necesită evaluare, astfel cum se explică în secțiunea 1. Acestea sunt chestiuni de prezentare și nu constituie, în sine, deficiențe de transpunere. **Recomandare** Revizuirea tabelelor de concordanță, astfel încât coloana 7 să se refere numai la proiectul de decizie, iar alte acte să fie citate în coloana 9. Eliminarea informațiilor care nu au legătură cu dispozițiile UE, corectarea trimiterilor la alineat, precum și citarea și motivarea articolului 21 alineatul (5) din Decizia 2008/615/JAI a Consiliului și adăugarea unei scurte note privind articolele înlocuite de Regulamentul Prüm II sau de modificare a altor acte ale UE.	
	168	**2.2.6. Terminologie juridică și traducere** Versiunea în limba engleză utilizează trei acronime pentru punctul unic de contact (UCP, PUC și UPC) și două pentru punctele naționale de contact (NCP și PNC). Serviciul de Securitate și Informații este denumit „Serviciul de Informații și Securitate” la punctul 1.5 și în expunerea de motive. Titlul capitolului IX din anexa 2 este în limba română. Persoanele dispărute sunt denumite „persoane dispărute dezvăluite” și „persoane dispărute fără știri”. Punctul 9 din expunerea de motive se referă la termene de „8 ore/3 zile”. Deficiențele identificate pot fi clasificate ca traducere și terminologie juridică inexactă. **Recomandare** Efectuarea unei revizuiri terminologice a versiunii în limba engleză a proiectului de decizie și a expunerii de motive înainte de transmiterea către Comisia Europeană, inclusiv corectarea „8 ore”.	**Precizare** Recomandarea ține de aspectele legate de traducerea eronată.