



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), alin. (6) și alin. (7), art. 19 alin. (6), art. 22 alin. (2), art. 28 alin. (4), art. 29 alin. (3) și art. 42 alin. (4) din Legea privind cooperarea polițienească internațională (Monitorul Oficial al Republicii Moldova, nr. YYY - YYY, art. ZZZ), 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;

- 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;

- 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 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;

- 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 sau, după caz, pentru asigurarea conectivității tehnice securizate necesare schimbului de date, 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 al MAI*** – pentru domeniul evidențelor poliției cu caracter criminal, contravențional, datele nominale privind persoanele urmărite, dispărute sau implicate în activități infracționale, 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 al MAI*** – pentru domeniul evenimentelor majore cu dimensiune transfrontalieră;

1.4. ***Agencia Servicii Publice*** – pentru domeniul de date privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, date privind documentele de călătorie, vizele, titlurile de valoare, 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 teroriste;

1.6. ***Serviciul Tehnologia Informației și Securitate Cibernetică*** – în calitate de punct național de contact tehnic pentru rețeaua securizată S-TESTA, responsabil de asigurarea conectivității, funcționării, disponibilității și securității canalului național de comunicații utilizat pentru schimbul de date.

2. Se aprobă:

2.1. Regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații, conform anexei nr. 1;

2.2. Regulamentul de organizare și funcționare a Punctelor Naționale de Contact în scopul schimbului de date și informații, conform anexei nr. 2.

3. 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.

4. Prezenta hotărâre intră în vigoare la data intrării în vigoare a Legii privind cooperarea polițienească internațională.

Prim-ministru

Alexandru Munteanu

Contrasemnează:

Ministrul afacerilor interne

Daniella Misail-Nichitin

REGULAMENTUL **de organizare și funcționare a Punctului Unic de Contact în scopul schimbului** **de date și informații**

I. DISPOZIȚII GENERALE

1. Prezentul 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 (ADN, dactiloscopie, imagini faciale), date privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, evidențe ale poliției, datele nominale privind persoanele urmărite, dispărute sau implicate în activități infracționale, datele dactiloscopice, date care nu privesc persoanele și informații operative, documente de călătorie, vizele, titlurile de valoare, inclusiv a celor declarate false, furate sau pierdute, precum și date privind permisele de conducere.

2. Scopul prezentului Regulament este intensificarea cooperării polițienești internaționale pentru prevenirea, depistarea și investigarea infracțiunilor, precum și facilitarea căutării persoanelor dispărute și identificarea rămășițelor umane.

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

4. În scopul transpunerii Directivei (UE) 2023/977, funcțiile de punct unic de contact pentru cooperarea polițienească internațională (*Single Point of Contact, în continuare – SPOC*) sunt exercitate de către PUC.

5. Prezentului Regulament, i se aplică noțiunile din Legea privind cooperarea polițienească internațională, precum și noțiunile utilizate cu următoarele semnificații:

5.1. *autoritate de aplicare a legii desemnată* – orice autoritate competentă de aplicare a legii, în sensul Legii privind cooperarea polițienească internațională, 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;

5.2. *Computer Emergency Response Team for the European Union institutions, bodies and agencies (în continuare – CERT-UE)* – centrul de răspuns la incidente cibernetice al instituțiilor, organele și agențiilor Uniunii Europene, recunoscut ca autoritate de sprijin operațional în domeniul securității informaționale la nivelul UE;

5.3. *Common Identity Repository (în continuare – CIR)* – 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;

5.4. *Common Repository for Reporting and Statistics (în continuare – CRRS)* – 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;

5.5. *European Search Portal (în continuare – ESP)* – 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;

5.6. *European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (în continuare – eu-LISA)* – 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;

5.7. *marcarea datelor* – procedura de aplicare a unui indicator specific (marcaj) asupra datelor cu caracter personal a căror exactitate este contestată de persoana vizată, acțiune care este similară cu blocarea acestora, în scopul limitării utilizării acestora până la clarificarea situației și informării partenerilor internaționali cu privire la acest statut în cadrul schimbului de date;

5.8. *incident semnificativ de securitate cibernetică* – orice eveniment care are sau poate avea un impact major asupra funcționării infrastructurii Router-ului ori a sistemului EPRIS sau care periclitizează disponibilitatea, integritatea și confidențialitatea datelor biometrice ori alfanumerice prelucrate, fiind de natură să cauzeze pierderi de date sau accesări neautorizate și să necesite notificarea partenerilor internaționali;

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

5.10. *informații direct accesibile* – acele informații pe care personalul SPOC 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 SIS);

5.11. *informații indirect accesibile* – datele care nu se află în sistemele interconectate ale SPOC și necesită o solicitare către alte autorități publice (ex: fisc, vamă) sau sectorul privat (ex: furnizori de servicii), fără dispunerea aplicării măsurilor coercitive, conform dreptului național;

5.12. *Single Point of Contact (în continuare – SPOC)* – structură administrativă și operațională desemnată la nivel național pentru a asigura fluxul informațional securizat cu statele membre ale Uniunii Europene și organizațiile internaționale profilate pe schimbul de informații de natură infracțională;

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

5.14. *Secure Trans European Services for Telematics between Administrations (în continuare – S-TESTA)* – 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.

II. STRUCTURA ȘI MODUL DE ORGANIZARE ȘI FUNCȚIONARE AL PUNCTULUI UNIC DE CONTACT

Secțiunea 1

Principiile de activitate ale PUC

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

6.1. *legalitatea, respectarea dreptului internațional și a tratatelor internaționale la care Republica Moldova este parte* - activitatea se desfășoară strict conform Legii privind cooperarea polițienească internațională și tratatelor internaționale, fără a afecta suveranitatea sau securitatea națională;

6.2. *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 personale;

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

6.4. *controlul ierarhic permanent, răspunderea personală și profesionalismul* - deciziile nu sunt pur automatizate, orice rezultat este verificat manual de personal calificat, care poartă răspundere personală pentru validitatea datelor;

6.5. *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.

7. În exercitarea atribuțiilor specifice privind căutarea și schimbul de date, PUC aplică principii operaționale prevăzute la art. 4 din Legea privind cooperarea polițienească internațională.

Secțiunea a 2-a

Structura organizatorică a PUC

8. 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.

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

9.1. *Secția Europol* – asigură schimbul de date și informații prin intermediul Router-ului și al sistemului EPRIS;

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

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

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

9.5. *Biroul național SIRENE* – gestionează și coordonează alertele în cadrul Sistemului de Informații Schengen (SIS), 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

10. PUC acționează ca interfață unică și centralizată între sistemele informaționale naționale și infrastructura centrală a Uniunii Europene, fiind structura administrativă și operațională desemnată la nivel național pentru a asigura fluxul informațional securizat cu statele membre ale Uniunii Europene, alte state și organizațiile internaționale profilate pe schimbul de date și informații de natură infracțională, având următoarele atribuții funcționale și operaționale principale:

10.1. asigurarea notificării oficiale către Secretariatul General al Consiliului Uniunii Europene și Comisiei Europene, în termen de cel mult o lună de la data desemnării, cu privire la desemnarea PUC și a Punctelor Naționale de Contact (în continuare – PNC) pe domenii de competență, precum și a listei limbilor stabilite pentru schimbul de informații conform pct. 39, inclusiv a oricăror modificări ulterioare ale acestora, în vederea publicării în Jurnalul Oficial al Uniunii Europene sau pe platformele online dedicate ale Comisiei;

10.2. 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;

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

10.4. coordonarea operativă a schimbului de profiluri ADN, date dactiloscopice și imagini faciale prin intermediul Router-ului UE, facilitând fluxul informațional între partenerii internaționali și CTCEJ;

10.5. realizarea schimbului de date și informații prin sistemul EPRIS, prin utilizarea instrumentului de căutare pentru interogarea registrelor naționale de evidențe ale poliției, datele nominale privind persoanele urmărite, dispărute sau implicate în activități infracționale, precum și pentru datele dactiloscopice;

10.6. efectuarea schimbului de date și informații prin sistemul EUCARIS pentru informațiile privind mijloacele de transport;

10.7. gestionarea operativă a alertelor în Sistemul de Informații Schengen (SIS) 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;

10.8. realizarea schimbului operativ de date prin interfața cu baza de date SLTD a Interpol, în vederea verificării documentelor de călătorie, vizele, titlurile de valoare, inclusiv a celor declarate false, furate sau pierdute, pe baza informațiilor puse la dispoziție de autoritățile competente;

10.9. gestionarea procedurilor de dare în urmărire internațională, localizarea persoanelor dispărute fără veste în contextul cauzelor penale sau din motive umanitare, identificarea rămășițelor umane și gestionarea procedurilor de predare/preluare a persoanelor;

10.10. asigurarea accesului efectiv al personalului desemnat pentru cooperarea cu Europol la toate bazele de date naționale relevante, în limitele competențelor legale, pentru a permite schimbul rapid de date și informații privind infracțiunile transfrontaliere, cu accent pe traficul ilicit de vehicule;

10.11. asigurarea suportului pentru operațiuni comune, supravegheri și urmăriri transfrontaliere, precum și gestionarea procedurilor de dare în urmărire internațională, localizare și de predare/preluare a persoanelor urmărite sau dispărute;

10.12. 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.

11. 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:

11.1. 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;

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

11.3. 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;

11.4. 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.

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

12.1. 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;

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

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

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

12.5. 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

13. 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.

14. Asigurarea conectivității tehnice, disponibilității și securității rețelei naționale de comunicații utilizate pentru conectarea la infrastructura externă aferentă schimbului de date și informații se realizează de către Serviciul Tehnologia Informației și Securitate Cibernetică (în continuare – STISC), în condițiile cadrului normativ.

15. Toate operațiunile de acces și schimb de date și informații sunt înregistrate în Sistemul electronic unic de gestionare a cazurilor, care asigură trasabilitatea acțiunilor de prelucrare și interoperabilitatea cu SIENA.

Secțiunea a 5-a

Condiții pentru solicitarea și schimbul de informații

16. PUC asigură faptul că orice cerere de informații transmisă către un 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.

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

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

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

17.3. 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.

18. Cererile de informații transmise de PUC trebuie să fie complet documentate și să conțină cel puțin următoarele elemente:

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

18.2. scopul și justificarea: descrierea detaliată a scopului cererii, a faptelor investigate și a modului de operare, cu indicarea infracțiunii vizate (pregătite sau comise);

18.3. obiectul cererii: precizarea detaliată a informațiilor solicitate și a legăturii de cauzalitate dintre scopul solicitării și persoana sau entitatea vizată;

18.4. datele de identificare: datele cu caracter personal ale persoanelor implicate, extrase conform actelor de identitate (nume, prenume, data nașterii, cetățenie, serie/număr act);

18.5. regimul de urgență: precizarea caracterului de urgență (dacă este cazul) și motivarea obiectivă a acestuia, indicând riscul iminent pentru viața persoanelor sau riscul pierderii relevanței probatorii;

18.6. localizarea datelor: motivele obiective pentru care se consideră că statul solicitat deține informațiile.

19. 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, 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 celui alt stat membru al Uniunii Europene sau alt stat.

20. Prin derogare de la pct. 19, 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:

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

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

20.3. siguranța unei persoane.

21. 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 subzistă.

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

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

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

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

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

Secțiunea a 6-a

Termene de furnizare a informațiilor și autorizarea judiciară

23. PUC furnizează informațiile solicitate în următoarele termene maxime:

23.1. **8 ore** pentru cereri urgente referitoare la informații direct accesibile;

23.2. **3 zile calendaristice** pentru cereri urgente referitoare la informații indirect accesibile;

23.3. **7 zile calendaristice** pentru toate celelalte cereri.

24. Flexibilitatea termenelor în funcție de complexitate: În cazuri excepționale, când cererea vizează un volum mare de date, necesită coordonarea cu multiple autorități furnizoare sau implică verificări transfrontaliere complexe, PUC poate prelungi termenele prevăzute la pct. 23.

25. În situația în care termenele nu pot fi respectate din cauza complexității cererii sau a necesității unei autorizări judiciare, PUC aplică următoarele măsuri:

25.1. informează imediat autoritatea solicitantă despre întârziere, precizând motivele obiective (tehnice, juridice sau de complexitate) și furnizând o estimare a noului termen de răspuns;

25.2. menține comunicarea constantă cu solicitantul, furnizând informațiile parțial, pe măsură ce acestea devin disponibile;

25.3. înregistrează justificarea prelungirii în Sistemul electronic unic de gestionare a cazurilor pentru audit și raportare statistică

26. În cazul în care legislația națională impune o autorizație judiciară pentru furnizarea informațiilor, PUC poate deroga de la termenele prevăzute la pct. 23, cu respectarea următoarelor condiții:

26.1. nu se solicită autorizație judiciară pentru furnizarea de informații către un alt stat membru dacă dreptul intern nu impune o astfel de procedură pentru furnizarea de informații similare în context național;

26.2. PUC sau autoritățile de aplicare a legii desemnate iau imediat toate măsurile necesare, conform dreptului intern, pentru a obține autorizația judiciară în cel mai scurt timp posibil;

26.3. examinarea cererilor de autorizare judiciară se realizează prin mecanisme de permanență (24/7), astfel încât să fie garantată respectarea termenelor de urgență prevăzute de prezentul Regulament;

26.4. PUC informează imediat autoritatea solicitantă despre întârzierea preconizată, precizând motivele și durata estimată a acesteia;

26.5. pe parcursul procedurii, PUC menține informată autoritatea solicitantă și furnizează informațiile imediat după obținerea autorizației judiciare;

26.6. cererile de autorizare sunt evaluate și soluționate în conformitate cu dreptul intern al statului membru al autorității judiciare competente;

26.7. autoritățile naționale asigură transmiterea informațiilor solicitate de PUC, cu respectarea termenelor prevăzute la pct. 23, pentru a permite încadrarea în limitele de timp impuse de standardele internaționale;

26.8. 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 alte canale autorizate în termen de cel mult 24 de ore.

Secțiunea a 7-a

Refuzul cererilor și furnizarea din proprie inițiativă

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

27.1. informațiile nu sunt disponibile sau cererea nu îndeplinește cerințele de necesitate și proporționalitate, prevăzute la pct. 17 din prezentul Regulament;

27.2. autorizația judiciară necesară a fost refuzată;

27.3. furnizarea datelor ar periclita interesele esențiale ale securității naționale, buna desfășurare a unei investigații în curs sau siguranța unei persoane sau ar prejudicia interesele importante protejate ale unei persoane juridice;

27.4. cererea vizează o infracțiune pedepsită cu maximum un an de închisoare conform dreptului intern sau o faptă care nu constituie infracțiune;

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

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

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

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

28. 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.

29. 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:

29.1. notificarea imediată: PUC informează autoritatea solicitantă în termenele prevăzute la pct. 23 despre imposibilitatea furnizării, precizând clar motivele refuzului sau natura defecțiunii tehnice;

29.2. 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);

29.3. 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;

29.4. orice notificare de refuz sau comunicare aferentă se transmite în limba în care a fost primită cererea, conform regulilor de la pct. 39.

30. 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 ar trebui refuzată.

31. Termenele de furnizare a informațiilor prevăzute la pct. 23 se suspendă din momentul în care autoritatea solicitantă primește cererea de clarificări, până în momentul în care clarificările solicitate sunt furnizate către PUC.

32. 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.

33. Informațiile furnizate prin PUC nu pot fi utilizate ca mijloace de probă în procedurile judiciare fără acordul prealabil al statului care le-a furnizat.

Secțiunea a 8-a

Cerințe operaționale și managementul datelor

34. 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 riguroasă a legislației privind protecția datelor cu caracter personal și a normelor speciale privind securitatea informațiilor cu accesibilitate limitată.

35. 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 S-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 de către PNC tehnic (STISC), în conformitate cu cerințele tehnice europene.

36. PUC este autoritatea responsabilă de decizia privind canalul de cooperare utilizat pentru schimbul de informații, având competența de a autoriza utilizarea altor canale securizate (Interpol, SELEC sau canale bilaterale) în funcție de disponibilitatea tehnică a partenerilor, cerințele de interoperabilitate și necesitatea asigurării eficienței schimbului, fără a afecta securitatea și integritatea datelor, luând în considerare următoarele situații și criterii:

36.1. necesitatea interoperabilității, în cazul în care statul membru partener sau țara terță nu utilizează canalul SIENA sau invocă lipsa acordurilor tehnice necesare;

36.2. implicarea unor țări terțe sau a organizațiilor internaționale care utilizează platforme de comunicare specifice (ex. Interpol, SELEC);

36.3. urgența majoră care impune utilizarea temporară a celui mai rapid canal disponibil pentru salvarea vieții sau integrității unei persoane;

36.4. existența unui incident tehnic neașteptat care împiedică utilizarea temporară a SIENA;

36.5. eficiența schimbului, atunci când natura datelor sau specificul canalului (ex: SELEC pentru criminalitatea organizată în regiune) garantează un rezultat operativ superior fără a afecta securitatea datelor.

37. Toate operațiunile PUC sunt înregistrate într-un sistem electronic unic de gestionare a cazurilor, care trebuie să respecte următoarele reguli:

37.1. înregistrările (log-urile) sunt păstrate timp de 3 ani pentru monitorizarea legalității;

37.2. conține date cu caracter personal doar atât timp cât este necesar și proporțional pentru îndeplinirea sarcinilor;

37.3. asigură ștergerea irevocabilă a datelor care nu mai sunt necesare;

37.4. este supus unei reexaminări privind necesitatea păstrării datelor în termen de cel mult 6 luni de la încheierea schimbului de informații.

38. 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.

39. 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.

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

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

40.2. categoriile de date furnizate sunt limitate strict la cele enumerate în secțiunea B din anexa II la Regulamentul (UE) 2016/794 privind Europol și sunt transmise doar dacă sunt necesare și proporționale cu scopul cererii;

40.3. 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.

41. În cazul în care o copie a unei cereri de informații sau a informațiilor furnizate este transmisă către Europol, PUC se asigură că scopurile prelucrării și orice restricții privind prelucrarea respectivă, conform standardelor prevăzute la pct. 40, sunt comunicate în mod corespunzător agenției.

42. 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

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

44. Arhitectura tehnică utilizată de PUC prin intermediul Router-ului este alcătuită din următoarele elemente componente, administrate tehnic de către Punctul Național de Contact tehnic:

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

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

44.3. infrastructura de comunicații securizată care asigură legătura cu ESP.

45. 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 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.

Secțiunea a 2-a

Sistemul european de inventariere a evidențelor poliției (EPRIS)

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

47. Sistemul EPRIS, pus la dispoziția PUC de către STI al MAI, include:

47.1. o infrastructură descentralizată instalată la nivel național;

47.2. un instrument de căutare ce permite interogarea simultană a registrelor naționale;

47.3. un canal de comunicații securizat.

48. 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)

49. 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.

50. 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, ASP, CTC-EJ), în etapa de operare a sistemelor proprii.

51. Orice incident tehnic, defecțiune a infrastructurii hardware sau software ori eroare de conectivitate a Router-ului, EPRIS sau a canalelor S-TESTA va fi raportat imediat de către PUC către PNC-urile tehnice responsabile, acesta din urmă având obligația restabilirii funcționării sistemelor.

IV. PROCEDURI OPERAȚIONALE ȘI INTEROPERABILITATE

Secțiunea 1

Proceduri de interogare și interoperabilitate cu sistemele Uniunii Europene

52. PUC este responsabil de lansarea 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 bănuț sau o victimă a unei infracțiuni de terorism ori a unei alte infracțiuni grave sunt stocate în respectivul registru.

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

54. 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.

55. 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.

56. 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.

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

58. 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.

59. Solicitățile 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.

60. 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.

61. 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.

62. 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 desfășoară în conformitate cu normele Regulamentului (UE) 2016/794 privind Europol.

63. 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

64. În scopul efectuării de căutări în registrele naționale ale evidențelor poliției prin intermediul EPRIS, în vederea identificării persoanelor urmărite, dispărute sau implicate în activități infracționale, PUC utilizează cel puțin două dintre următoarele date:

- 64.1. prenumele;
- 64.2. numele;
- 64.3. data nașterii.

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

- 65.1. pseudonimul (sau numele utilizat anterior);
- 65.2. cetățenia;
- 65.3. țara nașterii;
- 65.4. genul.

66. 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.

67. 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.

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

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

70. 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.

71. 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.

72. 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.

73. Specificațiile tehnice pentru procedura de interogare prin EPRIS, formatul răspunsurilor și numărul maxim al acestora sunt conforme cu actele de punere în aplicare ale Uniunii Europene.

Secțiunea a 3-a

Proceduri specifice pentru Sistemul EUCARIS

74. 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 pentru menținerea siguranței publice.

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

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

75.2. 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.

Secțiunea a 4-a

Confirmarea concordanțelor și schimbul setului de date de bază

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

77. Orice concordanță identificată este supusă unei revizuii manuale de către cel puțin un membru calificat al personalului, în scopul confirmării validității acesteia pe baza datelor de referință primite.

78. 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:

78.1. concordanța a fost confirmată manual conform pct. 77;

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

79. Prin derogare de la pct. 78, 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.

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

- 80.1. numele, prenumele;
- 80.2. data nașterii;
- 80.3. pseudonimele;
- 80.4. cetățenia;
- 80.5. locul și țara nașterii;
- 80.6. genul;
- 80.7. data și locul obținerii datelor biometrice;
- 80.8. infracțiunea aferentă;
- 80.9. numărul cauzei penale;
- 80.10. autoritatea responsabilă.

81. 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.

82. 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

83. 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.

84. 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.

85. 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

86. 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.

87. 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.

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

V. MANAGEMENTUL DATELOR, SECURITATEA ȘI JURNALIZAREA

Secțiunea 1

Securitatea sistemelor și a prelucrării datelor

89. 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.

90. Prelucrarea datelor cu caracter personal se realizează în conformitate cu legislația națională privind protecția datelor și cu standardele Uniunii Europene aplicabile în domeniul cooperării polițienești.

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

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

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

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

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

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

92. 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)

93. 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 art. 40 din Legea privind cooperarea polițienească internațională, care se păstrează pentru termenul special stabilit de acestea. La expirarea termenului de păstrare, datele înregistrate se șterg imediat.

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

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

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

- 94.3. sistemele de informații și bazele de date interogate;
- 94.4. identificatorul unic al persoanei autorizate care a efectuat sau a solicitat căutarea;
- 94.5. justificarea interogării, inclusiv numărul de referință al dosarului sau al cauzei penale
- 94.6. statutul persoanei vizate de interogare (bănuț, învinuit, condamnat, victimă, persoană dispărută fără veste, cadavru sau părțile acestuia), conform art. 42 alin. (2) din Legea privind cooperarea polițienească internațională.
- 95. 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 marcarea a datelor

- 96. În cazul constatării furnizării unor date incorecte, neactuale sau care nu ar fi trebuit furnizate, PUC notifică imediat autoritatea destinatară, asigurând corectarea sau ștergerea acestora fără întârzieri nejustificate.
- 97. 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.
- 98. 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.
- 99. 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.
- 100. 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.
- 101. Datele cu caracter personal primite sau furnizate legal de către PUC se șterg din evidențele sale operative:
 - 101.1. imediat ce se constată că nu mai sunt necesare pentru scopul pentru care au fost schimbate;
 - 101.2. la primirea unei notificări de la Punctul Național de Contact (PNC) privind expirarea termenului de păstrare în registrul sursă, conform legislației naționale;
 - 101.3. după expirarea perioadei maxime de păstrare prevăzute în Regulamentul (UE) 2016/794 privind Europol, pentru datele schimbate prin acest canal.

102. PUC reexaminează necesitatea păstrării datelor în termen de cel mult 6 luni de la încheierea schimbului de informații, asigurând ștergerea irevocabilă a celor care nu mai sunt necesare.

Secțiunea a 4-a

Automonitorizarea și protecția persoanelor vizate

103. PUC, în cooperare cu autoritățile competente care au dreptul de a utiliza cadrul Prüm II, implementează măsuri de automonitorizare pentru a verifica conformitatea tuturor activităților de prelucrare cu legislația privind protecția datelor cu caracter personal. Aceste măsuri includ revizuirea periodică a înregistrărilor (log-urilor) și a justificărilor legale introduse în Sistemul electronic unic de gestionare a cazurilor, pentru a asigura trasabilitatea deplină a fiecărui schimb de date și informații.

104. Centrul Național pentru Protecția Datelor cu Caracter Personal (*în continuare* – CNPDCP) exercită controlul asupra prelucrărilor efectuate de PUC și PNC, cooperând activ cu Autoritatea Europeană pentru Protecția Datelor (AEPD) în cadrul responsabilităților lor de supraveghere a Router-ului și a sistemului EPRIS.

105. 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.

106. 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.

107. 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 în vigoare.

Secțiunea a 5-a

Răspunderea juridică

108. Încălcarea normelor privind securitatea sistemelor, jurnalizarea operațiunilor sau prelucrarea datelor cu caracter personal stabilite în prezentul Regulament atrage răspunderea disciplinară, contravențională sau penală a personalului vinovat.

109. Constituie abateri grave sancționate conform legislației speciale, următoarele fapte:

109.1. accesul neautorizat la segmentele de infrastructură națională (Router, EPRIS, EUCARIS) sau la înregistrările (log-urile) de sistem;

109.2. utilizarea datelor primite în alte scopuri decât cele de cooperare polițienească sau în vederea identificării/re-identificării persoanelor în afara cadrului legal;

109.3. divulgarea informațiilor către autorități sau state terțe fără acordul prealabil al furnizorului inițial, cu încălcarea principiului controlului asupra difuzării ulterioare.

110. Tipurile de răspundere se aplică după cum urmează:

110.1. **răspunderea disciplinară** – se aplică personalului autorizat din cadrul PUC în conformitate cu statutul juridic al acestuia și legislația care reglementează activitatea fiecărei autorități în parte, pentru nerespectarea regimului de confidențialitate și a procedurilor de operare;

110.2. **răspunderea contravențională** – se stabilește în conformitate cu prevederile Codului Contravențional al Republicii Moldova pentru încălcarea regulilor de prelucrare a datelor cu caracter personal și a măsurilor de securitate a sistemelor informatice;

110.3. **răspunderea penală** – intervine în cazurile în care fapta întrunește elementele unei infracțiuni prevăzute de Codul Penal, referitoare la accesul neautorizat la informația computerizată sau abuzul de serviciu care a generat compromiterea integrității informațiilor internaționale.

VI. RAPORTARE ȘI INDICATORI STATISTICI

Secțiunea 1

Colectarea și furnizarea datelor statistice

111. În scopul evaluării eficienței cooperării polițienești internaționale, monitorizării legale și auditului securității, autoritățile competente/punctele naționale de contact, 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.

112. 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.

113. Această raportare vizează exclusiv managementul informațiilor și cuprinde:

113.1. numărul de cereri de informații transmise și primite;

113.2. numărul de răspunsuri furnizate, defalcate în cereri urgente și neurgente;

113.3. numărul de cereri refuzate și motivele aferente;

113.4. statisticile privind respectarea termenelor de 8 ore/3 zile/7 zile și impactul autorizațiilor judiciare asupra acestora.

114. 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 specifici pentru Router

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

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

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

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

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

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

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

115.7. tipul concordanțelor identificate, clasificate astfel:

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

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

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

115.7.4. date identificate (persoană) – date identificate (persoană).

Secțiunea a 3-a

Indicatori specifici pentru sistemele EPRIS și EUCARIS

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

116.1. numărul de interogări lansate și primite de către autoritățile competente naționale;

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

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

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

117.1. numărul total de interogări lansate de PUC și primite de la statele membre ori Europol;

117.2. numărul de interogări în fiecare dintre bazele de date conectate;

117.3. numărul de concordanțe obținute în urma interogărilor.

Secțiunea a 4-a

Utilizarea și protecția rapoartelor statistice

118. 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.

119. Datele statistice colectate sunt stocate după cum urmează:

119.1. indicatorii referitori la Router sunt transmiși și stocați în Registrul central de raportare și statistici (CRRS) gestionat de eu-LISA;

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

120. 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.

REGULAMENTUL

de organizare și funcționare a Punctelor Naționale de Contact în scopul schimbului de date și informații

I. DISPOZIȚII GENERALE

1. Prezentul 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 (ADN, dactiloscopie, imagini faciale), date privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, evidențe ale poliției, date care nu privesc persoanele și informații operative, documente de călătorie, vizele, titlurile de valoare, inclusiv a celor declarate false, furate sau pierdute, precum și date privind permisele de conducere.

2. Punctele Naționale de Contact (*în continuare – PNC*) sunt autoritățile 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 scopul schimbului de date și informații, prevăzut în Anexa nr. 1.

4. În sensul prezentului Regulament, se desemnează următoarele autorități în calitate de PNC, 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 (în continuare – STI) al MAI*** — pentru domeniul evidențelor poliției cu caracter criminal, contravențional, datele nominale privind persoanele urmărite, dispărute sau implicate în activități infracționale, 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 al 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 referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, date privind documente de călătorie, vizele, titlurile de valoare, 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 teroriste;

4.6. ***Serviciul Tehnologia Informației și Securitate Cibernetică (în continuare – STISC)*** – în calitate de punct național de contact tehnic pentru rețeaua securizată S-TESTA, responsabil de asigurarea conectivității, funcționării, disponibilității și securității canalului național de comunicații utilizat pentru schimbul de date.

5. PNC au obligația de a asigura interoperabilitatea sistemelor proprii cu infrastructura națională de comunicații securizate administrată de către Punctul Național de Contact tehnic (STISC), utilizând standardul privind formatul universal pentru mesaje (*în continuare – UMF*).

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 PUNCTELOR NAȚIONALE DE CONTACT 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 principii operaționale prevăzute la art. 4 din Legea privind cooperarea polițienească internațională.

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 expert 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 re-evalua și corecta setul de date în cel mai scurt timp.

Secțiunea a 3-a

Interfețele tehnice pentru schimbul de date

11. Schimbul de date, inclusiv automatizat dintre PNC și PUC se realizează prin intermediul următoarelor interfețe tehnice, în funcție de domeniul de competență specific:

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 S-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 (ROUTER, EPRIS ȘI UMF)

Secțiunea 1

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

13. PNC conform ariilor 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 S-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 al MAI, 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 funcției de administrare a EPRIS, STI asigură:

17.1. funcționarea neîntreruptă a instrumentului de căutare care permite interogarea simultană a registrelor de evidență;

17.2. securitatea tehnică a nodului EPRIS și a canalului de comunicații securizat între infrastructura centrală a Uniunii Europene și Republica Moldova;

17.3. pseudonimizarea tehnică a datelor nominative (nume, prenume) prin serii alfanumerice în etapa de căutare, pentru a proteja identitatea persoanelor.

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. Punctele Naționale de Contact, 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 dreptul intern al Republicii Moldova, informând PUC cu privire la aceste termene la momentul furnizării.

Secțiunea a 2-a

Procedura de marcarea datelor contestate

28. PNC asigură exactitatea și relevanța datelor cu caracter personal prelucrate.

29. Dacă o persoană vizată contestă exactitatea datelor deținute de un PNC, iar aceasta nu poate fi stabilită imediat, PNC-ul aplică un indicator de marcarea (marcaj) asupra datelor respective.

30. Marcajul limitează utilizarea datelor până la clarificarea situației și poate fi eliminat doar:

30.1. cu acordul expres al persoanei vizate;

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

30.3. în baza unei decizii a Centrului Național pentru Protecția Datelor cu Caracter Personal.

Secțiunea a 3-a

Automonitorizarea și protecția persoanelor vizate

31. În calitate de operatori de date, Punctele Naționale de Contact 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.

32. 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.

33. 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)

34. Fiecare PNC 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 art. 40 din Legea privind cooperarea polițienească internațională, care se păstrează pentru termenul special stabilit de acestea. La expirarea termenului de păstrare, datele înregistrate se șterg imediat.

35. Înregistrările trebuie să conțină: entitatea solicitantă, data și ora exactă, bazele de date interogate, identificatorul persoanei autorizate care a efectuat căutarea și justificarea interogării (referința la cazul penal).

Secțiunea a 2-a

Furnizarea indicatorilor statistici

36. PNC colectează și furnizează periodic către PUC datele necesare pentru elaborarea rapoartelor statistice cerute de Regulamentul (UE) 2024/982, fără a permite identificarea persoanelor vizate.

37. 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

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

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

38.2. *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;

38.3. *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.

39. 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.

40. Încălcarea normelor privind securitatea sistemelor, prelucrarea datelor cu caracter personal sau procedurile de validare manuală stabilite de prezentul Regulament atrage răspunderea disciplinară, contravențională sau penală a personalului desemnat din cadrul PNC, în conformitate cu legislația în vigoare.

41. Constituie abateri grave sancționate conform legislației speciale, următoarele fapte:

41.1. accesul neautorizat la bazele de date sectoriale (biometrice, mijloace de transport, evidențe ale poliției) prin intermediul interfețelor de schimb automatizat sau la înregistrările (log-urile) de sistem gestionate de PNC;

41.2. validarea eronată sau abuzivă a concordanțelor (hit-urilor), prin nerespectarea principiului intervenției umane sau a standardelor minime de calitate, generând riscul de identificare falsă a persoanelor;

41.3. nerespectarea obligației de marcare a datelor contestate sau de notificare a PUC în vederea rectificării/ștergerii datelor inexacte, fapt care aduce atingere exactității schimbului internațional de date și informații;

41.4. utilizarea datelor de referință accesate prin sistemele Prüm II în alte scopuri decât cele de cooperare polițienească sau pentru identificarea persoanelor în afara cadrului legal.

42. Tipurile de răspundere se aplică după cum urmează:

42.1. **răspunderea disciplinară** – se aplică personalului autorizat din cadrul PNC în conformitate cu statutul juridic al acestuia și legislația care reglementează activitatea fiecărei autorități în parte, pentru nerespectarea regimului de confidențialitate și a procedurilor de operare;

42.2. **răspunderea contravențională** – se stabilește în conformitate cu prevederile Codului Contravențional al Republicii Moldova pentru încălcarea regulilor de protecție a datelor cu caracter personal și a măsurilor de securitate a sistemelor informatice;

42.3. **răspunderea penală** – intervine în cazurile în care fapta întrunește elementele unei infracțiuni prevăzute de Codul Penal, referitoare la accesul neautorizat la informația computerizată, abuzul de serviciu sau divulgarea datelor care permit re-identificarea persoanelor în afara procedurilor legale.

VII. Centrul tehnico-criminalistic și expertize judiciare al Inspectoratului General al Poliției

Secțiunea 1

Atribuțiile specifice în domeniul datelor biometrice

43. 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.

44. CTCEJ 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.

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 expert 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. CTCEJ stabilește, prin act administrativ, subdiviziunea structurală 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 confidentiale) 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 al Ministerului Afacerilor Interne

Secțiunea 1

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

49. STI al MAI este desemnat în calitate de PNC responsabil pentru domeniul evidențelor poliției cu caracter criminal, contravențional și dactiloscopic, având rolul de a gestiona registrele naționale și de a furniza PUC datele de referință necesare schimbului internațional de date și informații. În exercitarea acestor atribuții, STI asigură operarea tehnică și interconectarea infrastructurii descentralizate a sistemului EPRIS cu sistemele naționale de evidență (Sistemului Informațional Automatizat "Registrul Informației Criminalistice și Criminologice"),

permițând interogarea simultană a registrelor de evidență gestionate de către autoritățile competente din statele membre și Europol.

50. La primirea unei solicitări de interogare prin intermediul sistemului EPRIS, STI asigură, prin mecanisme automatizate și fără întârziere, lansarea 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.

Secțiunea a 2-a

Standarde tehnice și protecția datelor în sistemul EPRIS

51. În scopul protejării identității persoanelor vizate în etapa de căutare, STI are obligația de a asigura pseudonimizarea 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.

52. 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.

Secțiunea a 3-a

Organizarea internă, jurnalizarea și raportarea

53. 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 confidentiale, pentru a preveni prelucrarea neautorizată a datelor.

54. STI asigură jurnalizarea obligatorie a tuturor operațiunilor de acces și schimb de date și informații pentru o perioadă de 3 ani, înregistrările conținând identificatorul persoanei autorizate și referința la ancheta penală specifică. STI colectează și transmite periodic către PUC indicatorii statistici referitori la numărul de interogări primite și lansate, precum și numărul de concordanțe pozitive identificate, asigurându-se că raportarea nu permite identificarea persoanelor vizate.

IX. Inspectoratul General de Carabinieri al Ministerului Afacerilor Interne

Secțiunea 1

Atribuțiile specifice în domeniul evenimentelor majore cu dimensiune transfrontalieră

55. IGC al MAI este desemnat în calitate de PNC responsabil pentru domeniul evenimentelor majore cu dimensiune transfrontalieră, având rolul de a

furniza și de a schimba informații cu PUC și entitățile similare din statele membre în scopul menținerii ordinii și siguranței publice. Aceste activități vizează prevenirea, depistarea și investigarea infracțiunilor, precum și gestionarea riscurilor asociate evenimentelor cu impact transfrontalier.

56. 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 din cadrul IGC, care operează prin intermediul canalelor Europol și al mecanismelor europene de cooperare polițienească.

57. 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.

Secțiunea a 2-a

Canale de comunicare și interoperabilitate tehnică

58. Pentru schimbul de informații aferente interogărilor sau solicitărilor primite, IGC utilizează ca interfață principală de comunicare SIENA, sub coordonarea operativă a PUC. IGC are obligația de a asigura interoperabilitatea sistemelor proprii de evidență cu infrastructura gestionată de PUC, utilizând standardul UMF pentru toate mesajele structurate transmise.

59. IGC are obligația de a asigura interoperabilitatea sistemelor proprii de evidență cu infrastructura gestionată de PUC, utilizând standardul 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 3-a

Organizarea administrativă, jurnalizarea și statistica

60. 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.

61. IGC asigură jurnalizarea operațiunilor de prelucrare a datelor pentru o perioadă de 3 ani, înregistrările trebuind să cuprindă justificarea legală a fiecărei interogări sau furnizări de date. Periodic, IGC transmite către PUC indicatorii statistici privind numărul de solicitări primite și soluționate, tipul evenimentelor vizate și rezultatele cooperării, fără a permite identificarea directă a persoanelor fizice vizate.

X. Agenția Servicii Publice

Secțiunea 1

Atribuțiile specifice în domeniul datelor privind mijloacele de transport, documentelor de călătorie și al permiselor de conducere

62. ASP este desemnată în calitate de PNC responsabil de gestionarea bazelor de date naționale privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, a datelor referitoare la documente de călătorie, vizele, titlurile de valoare, 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.

63. 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 (SIS) în toate cazurile de raportare a furtului certificatelor de înmatriculare a vehiculelor.

64. ASP asigură lansarea și primirea interogărilor automatizate fără întârziere, garantând accesul autorităților competente la datele privind proprietarii de vehicule și statutul documentelor de călătorie. 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.

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

66. 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.

Secțiunea a 2-a

Managementul calității datelor și securitatea prelucrării

67. 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. 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.

68. 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/Biroului național SIRENE pentru actualizarea corespunzătoare în Sistemul de Informații Schengen.

69. 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

70. ASP stabilește, prin act administrativ, subdiviziunea structurală responsabilă de executarea atribuțiilor de PNC și desemnează nominal persoanele autorizate să efectueze interogările și să gestioneze fluxul de date. Instituția asigură jurnalizarea obligatorie a tuturor operațiunilor de acces și schimb de date și informații pentru o perioadă de 3 ani, înregistrările incluzând identificatorul persoanei autorizate, bazele de date interogate și justificarea interogării.

71. 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 concordante 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 teroriste

72. SIS este desemnat în calitate de PNC responsabil pentru domeniul furnizării informațiilor necesare prevenirii infracțiunilor teroriste, exclusiv în cadrul mecanismului de schimb de date și informații reglementat de Regulamentul (UE) 2024/982. 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.

73. SIS asigură că furnizarea informațiilor se realizează cu respectarea strictă a principiilor necesității și proporționalității, vizând exclusiv prevenirea, depistarea și investigarea infracțiunilor de terorism. 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

74. 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 interfetei 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.

75. 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

76. 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.

77. SIS asigură jurnalizarea tuturor operațiunilor de acces și schimb de date și informații pentru o perioadă de 3 ani, înregistrările trebuind să conțină identificatorul persoanei autorizate și referința la cazul sau ancheta penală specifică. Periodic, SIS colectează și furnizează către PUC indicatorii statistici privind numărul de interogări lansate și primite, precum și concordanțele identificate, asigurându-se că raportarea nu permite identificarea directă a persoanelor vizate.

XII. Serviciul Tehnologia Informației și Securitate Cibernetică

Secțiunea 1

Atribuțiile specifice în calitate de Punct Național de Contact tehnic

78. STISC este desemnat în calitate de PNC tehnic pentru rețeaua securizată S-TESTA, fiind responsabil de asigurarea conectivității, funcționării, disponibilității și securității canalului național de comunicații utilizat pentru schimbul de date.

79. În exercitarea atribuțiilor sale, STISC îndeplinește următoarele funcții principale:

79.1. administrează la nivel național infrastructura securizată de comunicații S-TESTA, asigurând legătura tehnică între nodurile de comunicații ale PUC/PNC și infrastructura centrală a Uniunii Europene;

79.2. asigură suportul tehnic pentru conectarea și funcționarea Router-ului UE, a sistemului EPRIS și a sistemului EUCARIS, garantând transportul securizat al datelor pe segmentul național;

79.3. asigură conectivitatea tehnică și securitatea canalului național de comunicații necesar funcționării interfețelor de acces la Sistemul de Informații Schengen (SIS), în conformitate cu cerințele tehnice europene.

Secțiunea a 2-a

Securitatea cibernetică și managementul incidentelor

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

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

81.1. 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;

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

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

Secțiunea a 3-a

Organizarea internă și jurnalizarea operațiunilor tehnice

82. STISC stabilește, prin act administrativ intern, subdiviziunea responsabilă de administrarea tehnică a rețelei S-TESTA și desemnează personalul autorizat să gestioneze infrastructura de comunicații.

83. STISC asigură jurnalizarea operațiunilor tehnice de administrare a rețelei și a fluxurilor de date pe care le gestionează, păstrând înregistrările (log-urile) pentru o perioadă de 3 ani. Înregistrările vor cuprinde data, ora, starea conexiunii și identificatorul tehnic al administratorului care a efectuat intervenții asupra sistemelor de comunicații.

84. STISC colectează și furnizează periodic către PUC indicatorii tehnici privind disponibilitatea rețelei și performanța canalelor de comunicații, în scopul elaborării rapoartelor statistice și al monitorizării calității serviciilor de schimb de date și informații.

NOTA DE FUNDAMENTARE

la proiectul de hotărâri 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 de hotărâri 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), alin. (6) și alin. (7), art. 19 alin. (6), art. 22 alin. (2), art. 28 alin. (4), art. 29 alin. (3) și art. 42 alin. (4) din Legea privind cooperarea polițienească internațională (număr unic 264/MAI). Proiectul de hotărâri 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 hotărâri 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. 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; 4. Poziției comune 2005/69/JAI a Consiliului din 24 ianuarie 2005 privind schimbul de anumite date cu Interpol; 5. Deciziei 2004/919/CE a Consiliului din 22 decembrie 2004 privind combaterea criminalității referitoare la vehicule și având implicații transfrontaliere. Precizare: Necesitatea promovării și înregistrării prezentului proiect de hotărâre derivă din faptul că atât proiectul de lege, cât și proiectul de hotărâre constituie priorități de nivel I și urmează a fi transmise concomitent spre consultare Comisiei Europene, întrucât acestea asigură transpunerea integrală 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), și actele UE enumerate mai sus. După expunerea Comisiei Europene asupra proiectelor, se va respecta etapele de promovare prevăzute de Legea nr. 100/2017 cu privire la actele normative, adică, 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, va fi prezentat pentru aprobare Guvernului, după aprobarea proiectului de lege privind cooperarea polițienească internațională (număr unic 264/MAI).
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 hotărâri 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 suspectilor 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 Centrul Cooperare Polițienească Internațională (CCPI) 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 hotărâri 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 AND, 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.

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 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** - profiluri ADN, date dactiloscopice și imagini faciale;
- **Serviciul Tehnologii Informaționale al MAI** – pentru domeniul evidențe polițienești;
- **Inspectoratul General de Carabinieri al MAI** – pentru domeniul pentru evenimente majore;
- **Agenția Servicii Publice** – pentru domeniul de date privind înmatricularea vehiculelor, date privind pașapoarte furate sau pierdute și date privind permisele de conducere;
- **Serviciul de Informații și Securitate al Republicii Moldova** – pentru domeniul furnizării informațiilor necesare prevenirii infracțiunilor teroriste;
- **Serviciul Tehnologia Informației și Securitate Cibernetică** – în calitate de punct național de contact tehnic pentru rețeaua securizată S-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 hotărâri 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.

Deși Centrul 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, CNA, 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 (SPOC), 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).
3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare
Mentținerea 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
Sub aspect financiar, proiectul nu necesită cheltuieli suplimentare din bugetul de stat, cheltuielile se vor efectua din contul alocațiilor prevăzute în aceste scopuri în bugetele instituțiilor implicate, precum și din alte surse conform legislației. În calitate de puncte de contact vor fi desemnați reprezentanți ai autorităților publice, care pe lângă atribuțiile de bază, în baza fișelor de post și a Regulamentelor de activitate, vor asigura schimbul de informații potrivit domeniilor de activitate.
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 asupra prelucrării datelor cu caracter personal, întrucât instituie un cadru juridic pentru căutarea și schimbul de informații între autoritățile competente ale Republicii Moldova și autoritățile competente ale statelor membre, inclusiv prin mecanisme automatizate (profiluri ADN, date dactiloscopice, anumite date privind înmatricularea vehiculelor, imagini faciale, evidențe ale poliției), precum și prin schimburi neautomatizate în cazurile prevăzute de lege (evenimente majore cu dimensiune transfrontalieră, prevenirea infracțiunilor teroriste, identificarea persoanelor dispărute și a rămășițelor umane). Datele vizate sunt date cu un grad sporit de sensibilitate (în special date biometrice), iar operațiunile de prelucrare implică riscuri inerente privind accesul neautorizat, utilizarea în alte scopuri, erori de calitate a datelor, precum și riscuri de securitate informațională în context transfrontalier.

Impactul asupra datelor cu caracter personal este unul de securizare și responsabilizare. Deși crește volumul de date prelucrate prin mijloace automatizate, nivelul de protecție a acestora este ridicat la standarde europene, oferind cetățenilor garanții juridice și tehnice mult mai solide decât în sistemele de cooperare clasice.

În vederea reducerii acestor riscuri, proiectul instituie garanții juridice și organizatorice care limitează prelucrarea la scopuri determinate și legitime, impune condiții de acces și autorizare, stabilește obligații de confidențialitate, securitate și integritate a datelor, inclusiv utilizarea criptării și a măsurilor tehnice și organizatorice adecvate. Proiectul prevede, de asemenea, obligații de înregistrare și evidență a accesărilor și operațiunilor de prelucrare, păstrarea înregistrărilor pe termene determinate, utilizarea acestora exclusiv pentru monitorizarea protecției datelor, verificarea admisibilității și legalității prelucrării, precum și pentru asigurarea securității și integrității datelor. Sunt prevăzute reguli privind ștergerea datelor după atingerea scopului sau la expirarea termenelor stabilite, iar în cazul schimburilor în legătură cu evenimente majore se instituie termene maxime de păstrare.

Sunt instituite garanții stricte: prelucrarea datelor doar în scopurile prevăzute, limitarea categoriilor de date transmise la cele esențiale și jurnalizarea obligatorie a tuturor operațiunilor pentru o perioadă de 3 ani.

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 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), și 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, și a Deciziei 2004/919/CE a Consiliului din 22 decembrie 2004 privind combaterea criminalității referitoare la vehicule și având implicații transfrontaliere.
5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE Proiectul creează cadrul juridic intern necesar implementării cerințelor europene pentru aprobarea instrucțiunilor naționale pentru a defini în mod clar punctele naționale de contact (cum ar fi punctul național responsabil de gestionarea schimburilor automate: Prum privind datele dactiloscopice, imaginile faciale, profilurilor ADN și verificarea potențialei potriviri cu datele biometrice).
6. Avizarea și consultarea publică a proiectului În vederea respectării prevederilor Legii nr. 100/2017 cu privire la actele normative și Legii nr. 239/2008 privind transparența în procesul decizional, anunțul privind inițierea elaborării proiectului hotărârii Guvernului pentru aprobarea proiectului de lege pentru modificarea Legii nr. 288/2016 privind funcționarul public cu statut special din cadrul Ministerului Afacerilor Interne a fost plasat pe platforma guvernamentală www.particip.gov.md și este disponibil la link-ul: https://particip.gov.md/index.php/ru/document/stages/anunt-privind-initierea-procesului-de-elaborare-a-actului-normativcu-referire-la-instituirea-si-functionarea-punctului-unic-de-contact-si-apunctelor-nationale-de-contact-in-scopul-schimbului-automatizat-de-date/16606. Totodată, în conformitate cu prevederile Legii nr. 100/2017, proiectul de act normativ va fi remis spre avizare autorităților interesate și va fi supus consultărilor publice, iar în scopul respectării prevederilor Legii nr. 239/2008 privind transparența în procesul decizional, proiectul urmează a fi plasat pe pagina web oficială a Ministerului Afacerilor Interne (https://www.mai.gov.md), la compartimentul „Transparență”, rubrica „Consultări publice”, precum și pe platforma guvernamentală particip.gov.md.
7. Concluziile expertizelor Proiectul urmează a fi supus expertizei anticorupție, expertizei juridice și expertizei de compatibilitate cu legislația UE în conformitate cu art. 35, 36 și 37 din Legea nr. 100/2017 cu privire la actele normative.
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.
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 modificate fișele de post și Regulamentele de activitate ale subdiviziunilor/autorităților din cadrul cărora vor fi desemnate puncte de contact pentru schimbul de date și informații cu statele membre. Suplimentar acțiunilor de modificare a cadrului normativ intern, implementarea proiectului necesită realizarea instruirii personalului implicat în schimbul de informații

Ministrul afacerilor interne

Daniella MISAIL-NICHITIN

TABEL DE CONCORDANȚĂ

la proiectul de Hotărâre 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.	Titlul actului Uniunii Europene, inclusiv cele mai recente amendamente incluse: Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere			
2.	Titlul proiectului de act normativ național: Proiect de Hotărâre 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			
3.	Gradul general de compatibilitate Parțial compatibil			
4.	Autoritatea/persoana responsabilă Ministerul Afacerilor Interne			
5.	Data întocmirii/actualizării 18.05.2026			
6. Actul Uniunii Europene		7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observații
Articolul 1. Obiectiv și domeniu de aplicare Prin prezenta decizie, statele membre intenționează să accelereze cooperarea transfrontalieră în domeniile reglementate de titlul VI din tratat și, în special, schimbul de informații între autoritățile cu atribuții de prevenire și cercetare a infracțiunilor. În acest scop, prezenta decizie cuprinde norme în următoarele domenii: (b) dispoziții privind condițiile de furnizare de date privind evenimente majore care au o dimensiune transfrontalieră (capitolul 3); (c) dispoziții privind condițiile de furnizare a informațiilor pentru prevenirea infracțiunilor teroriste (capitolul 4); (d) dispoziții privind condițiile și procedura pentru intensificarea cooperării poliției la nivel transfrontalier prin diferite măsuri (capitolul 5).			Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 1. Obiectul de reglementare (2) Prezenta lege stabilește norme privind: d) schimbul de informații pentru gestionarea evenimentelor majore cu dimensiune transfrontalieră și pentru prevenirea infracțiunilor cu caracter terorist;

Articolul 2. Crearea fișierelor naționale de date ADN (1) Statele membre deschid și mențin fișiere naționale de date ADN în vederea cercetării infracțiunilor. În temeiul prezentei decizii, prelucrarea datelor înregistrate în aceste fișiere se efectuează în conformitate cu prezenta decizie, cu respectarea legislației naționale aplicabile procedurii respective de prelucrare. (2) În scopul aplicării prezentei decizii, statele membre asigură disponibilitatea datelor de referință din fișierele lor naționale de date ADN, astfel cum sunt menționate la alineatul (1) prima teză. Datele de referință conțin numai profilurile ADN create din partea necodată a ADN-ului, precum și un număr de identificare. Datele de referință nu conțin nicio dată care să permită identificarea directă a persoanei vizate. Datele de referință care nu sunt atribuite niciunei persoane („profiluri ADN neidentificate”) sunt recunoscute ca atare. (3) Fiecare stat membru informează Secretariatul General al Consiliului cu privire la fișierele naționale de date ADN cărora li se aplică articolele 2-6, precum și cu privire la condițiile de căutare automatizată prevăzute la articolul 3 alineatul (1), în conformitate cu articolul 36.	<i>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</i> Anexa nr.1 Punctul 10. PUC acționează ca interfață unică și centralizată între sistemele informaționale naționale și infrastructura centrală a Uniunii Europene, fiind structura administrativă și operațională desemnată la nivel național pentru a asigura fluxul informațional securizat cu statele membre ale Uniunii Europene, alte state și organizațiile internaționale profilate pe schimbul de date și informații de natură infracțională, având următoarele atribuții funcționale și operaționale principale: 10.1. asigurarea notificării oficiale către Secretariatul General al Consiliului Uniunii Europene și Comisiei Europene, în termen de cel mult o lună de la data desemnării, cu privire la desemnarea PUC și a Punctelor Naționale de Contact (în continuare – PNC) pe domenii de competență, precum și a listei limbilor stabilite pentru schimbul de informații conform pct. 39, inclusiv a oricăror modificări ulterioare ale acestora, în vederea publicării în Jurnalul Oficial al Uniunii Europene sau pe platformele online dedicate ale Comisiei; Anexa nr.2 Punctul 43. CTCEJ este autoritatea responsabilă de gestionarea și administrarea bazelor de date naționale privind profilurile	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 10. Date ADN de referință (1) Autoritatea competentă de aplicare a legii asigură punerea la dispoziție a profilurilor ADN stocate în Registrul de stat al datelor genetice, pentru efectuarea căutării automatizate în bazele de date de către autoritățile statelor membre ale Uniunii Europene și de Europol, în condițiile prezentei legi. (2) Datele de referință ADN puse la dispoziție nu conțin date care să permită identificarea directă a persoanei, iar profilurile ADN neidentificate se marchează distinct și sunt recunoscute ca atare în sistem. (3) Prelucrarea datelor de referință ADN se realizează în conformitate cu prevederile prezentei legi și cu respectarea procedurii de prelucrare a datelor respective în conformitate cu legislația privind protecția datelor cu caracter personal.

	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.		
Articolul 3. Căutarea automatizată a profilurilor ADN (1) În vederea cercetării infracțiunilor, statele membre autorizează punctele naționale de contact ale celorlalte state membre, astfel cum sunt menționate la articolul 6, să aibă acces la datele de referință în fișierele lor de date ADN, autorizându-le să efectueze căutări automatizate prin compararea profilurilor ADN. Căutările pot fi efectuate numai în cazuri individuale și în conformitate cu dreptul național al statului membru solicitant. (2) În cazul în care o căutare automatizată arată concordanța dintre un profil ADN furnizat și un profil ADN înregistrat în fișierul analizat al statului membru destinatar, punctul național de contact al statului membru care efectuează căutarea primește o notificare automatizată a datelor de referință în raport cu care a fost identificată o concordanță. Dacă nu poate fi identificată nicio concordanță, acest fapt se notifică automatizat.	<i>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</i> Anexa nr.1 Punctul 63. Căutările automatizate prevăzute în prezenta secțiune se efectuează exclusiv în cadrul unor cazuri individuale și în conformitate cu dreptul intern. Punctul 55. 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. Anexa nr.2 Punctul 43. este autoritatea responsabilă de gestionarea și administrarea bazelor de date naționale privind profilurile ADN,	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 11. Căutarea automatizată a profilurilor ADN (1) În scopul prevenirii, depistării și investigării infracțiunilor, la momentul primei conectări la infrastructura tehnică prevăzută de prezenta lege, punctul național de contact efectuează o comparare integrală a profilurilor ADN din Registrul de stat al datelor genetice cu profilurile ADN stocate în bazele de date ale statelor membre ale Uniunii Europene și ale Europol. (2) După realizarea conectării, punctul național de

	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. 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.	contact asigură căutarea automatizată prin compararea profilurilor ADN nou introduse în Registrul de stat al datelor genetice cu profilurile ADN stocate în bazele de date ADN ale altor state membre ale UE și cu datele Europol. (3) Dacă căutările automatizate menționate la alin. (2) nu pot fi efectuate, punctul național de contact poate conveni, la nivel bilateral, cu statul membru vizat sau cu Europol, efectuarea acestora într-o etapă ulterioară, prin compararea profilurilor ADN nou adăugate cu profilurile stocate în bazele de date ale statelor membre implicate sau ale Europol. (4) Căutările menționate la alin. (1)-(3) se efectuează exclusiv în cazuri individuale, cu respectarea prezentei legi și a normelor privind protecția datelor cu caracter personal. (5) În cazul identificării unei concordanțe („hit”) între un profil ADN transmis și un profil ADN stocat într-o bază de date a unui stat membru sau a statului membru solicitat, punctul național de

			contact primește o notificare automatizată care conține datele de referință ale profilului ADN corespunzător pentru care a fost identificată concordanța. (6) Notificarea automată a concordanței se generează numai dacă este întrunit pragul minim de loci stabilit potrivit cerințelor tehnice aplicabile. (7) Confirmarea concordanței între două profiluri ADN se realizează prin revizuire manuală de către un expert sau specialist în genetică judiciară din cadrul subdiviziunii responsabile de administrarea Registrului de stat al datelor genetice, calificat potrivit legislației naționale și procedurilor interne aplicabile. (8) În cazul în care confirmarea este realizată de autoritatea competentă de aplicare a legii a Republicii Moldova, punctul național de contact informează statul membru sau Europol cu privire la rezultatul revizuirii manuale.
Articolul 4. Compararea automatizată a profilurilor ADN	<i>Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului</i>	Compatibil	

(1) În vederea cercetării infracțiunilor, prin intermediul punctelor lor naționale de contact și de comun acord, statele membre compară profilurile lor ADN neidentificate cu toate profilurile ADN provenind din datele de referință ale altor fișiere naționale de date ADN. Furnizarea și compararea profilurilor se realizează în mod automatizat. Furnizarea profilurilor ADN neidentificate spre comparare nu se realizează decât în cazul în care este prevăzută de legislația națională a statului membru solicitant. (2) În cazul în care, ca rezultat al comparării menționate la alineatul (1), un stat membru constată că profilurile ADN furnizate concordă cu orice profil din propriile sale fișiere de date ADN, acesta comunică fără întârziere punctului național de contact al celui alt stat membru datele de referință pe baza cărora a fost constatată concordanța.	<i>Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații</i> Anexa nr.1 Punctul 43. În scopul facilitării stabilirii de conexiuni între Republica Moldova, statele membre ale Uniunii Europene și Europol, PUC utilizează Router-ul ca punct central de legătură pentru interogarea, extragerea și evaluarea automatizată a datelor biometrice, precum și pentru extragerea datelor alfanumerice. Punctul 53. La primirea unei solicitări de interogare din partea Router-ului, PUC, în calitate de autoritate a statului solicitat, asigură lansarea interogării în bazele de date naționale în mod automatizat și fără întârziere. Punctul 55. 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. Anexa nr.2 Punctul 43. 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.		
Articolul 5. Transmiterea de date suplimentare cu caracter personal și de alte informații În cazul în care procedurile menționate la articolele 3 și 4 indică o concordanță între profilurile ADN, furnizarea de date suplimentare cu caracter personal și de alte informații în legătură cu datele de referință se realizează în temeiul legislației naționale, inclusiv al dispozițiilor privind asistența judiciară, a statului membru solicitat.	<i>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</i> Anexa nr.1 Punctul 76. În cazul în care o căutare automatizată indică o concordanță (hit), PUC recepționează notificarea automatizată conținând datele de referință corespunzătoare. Punctul 77. Orice concordanță identificată este supusă unei revizuii manuale de către cel puțin un membru calificat al personalului, în scopul confirmării validității acesteia pe baza datelor de referință primite. Punctul 78. 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: 78.1. concordanța a fost confirmată manual conform pct. 77; 78.2. a fost transmisă o descriere a faptelor și a fost indicată infracțiunea subiacentă, utilizând tabelul comun al categoriilor de infracțiuni stabilit la nivelul	Compatibil	

	Uniunii Europene, în vederea evaluării proporționalității cererii în conformitate cu legislația națională. Punctul 79. Prin derogare de la pct. 78, 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. Punctul 80. În cazul datelor identificate, datele de bază cuprind, în măsura disponibilității: 80.1. numele, prenumele; 80.2. data nașterii; 80.3. pseudonimele; 80.4. cetățenia; 80.5. locul și țara nașterii; 80.6. genul; 80.7. data și locul obținerii datelor biometrice; 80.8. infracțiunea aferentă; 80.9. numărul cauzei penale; 80.10. autoritatea responsabilă. Punctul 81. 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. Punctul 82. 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.		
Articolul 6. Punctul național de contact și măsurile de punere în aplicare	<i>Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de</i>	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i>

(1) Fiecare stat membru desemnează un punct național de contact în scopul transmiterii datelor menționate la articolele 3 și 4. Competențele punctelor naționale de contact sunt reglementate de legislația națională aplicabilă. (2) Măsurile de punere în aplicare, astfel cum sunt menționate la articolul 33, stabilesc detaliile tehnice ale procedurilor menționate la articolele 3 și 4.	Contact în scopul schimbului de date și informații Punctul 1. Se desemnează următoarele autorități în calitate de Puncte Naționale de Contact, pe domenii de competență sau, după caz, pentru asigurarea conectivității tehnice securizate necesare schimbului de date, 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 al MAI – pentru domeniul evidențelor poliției cu caracter criminal, contravențional, datele nominale privind persoanele urmărite, dispărute sau implicate în activități infracționale, 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 al MAI – pentru domeniul evenimentelor majore cu dimensiune transfrontalieră;	Articolul 6. Punctul unic de contact și atribuțiile acestuia (1) Se desemnează în calitate de punct unic de contact pentru cooperarea polițienească internațională subdiviziunea specializată în cooperare polițienească internațională din subordinea Inspectoratului General al Poliției al Ministerului Afacerilor Interne. (2) Punctul unic de contact asigură cooperarea cu punctele naționale de contact desemnate prin hotărâre de Guvern, din cadrul autorităților competente naționale, pe următoarele domenii: a) profiluri ADN; (7) Organizarea, funcțiile și modul de funcționare a punctului unic de contact și a punctelor naționale de contact pe domeniile prevăzute la alin. (2), se stabilesc prin hotărâre de Guvern.

	1.4. Agenția Servicii Publice – pentru domeniul de date privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, date privind documentele de călătorie, vizele, titlurile de valoare, 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 teroriste; 1.6. Serviciul Tehnologia Informației și Securitate Cibernetică – în calitate de punct național de contact tehnic pentru rețeaua securizată S-TESTA, responsabil de asigurarea conectivității, funcționării, disponibilității și securității canalului național de comunicații utilizat pentru schimbul de date. Punctul 2. Se aprobă: 2.1. Regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații, conform anexei nr. 1; 2.2. Regulamentul de organizare și funcționare a Punctelor Naționale de Contact în scopul schimbului de date și informații, conform anexei nr. 2.		
 Articolul 7. Prelevarea de material biologic și transmiterea profilurilor ADN Atunci când, în cadrul unor cercetări sau al unor proceduri penale aflate în curs, lipsește profilul ADN al unei persoane determinate		Compatibil	 Proiectul de lege privind cooperarea polițienească internațională

care se găsește pe teritoriul statului membru solicitat, statul membru solicitat acordă asistență judiciară prin prelevarea și analizarea materialului biologic al persoanei respective, precum și prin furnizarea profilului ADN obținut, dacă: (a) statul membru solicitant comunică scopul pentru care această procedură este necesară; (b) statul membru solicitant prezintă un mandat de cercetare sau o declarație emisă de autoritatea competentă, astfel cum este prevăzut de legislația națională a statului membru respectiv, din care să rezulte că toate cerințele pentru prelevarea și analizarea materialului biologic ar fi îndeplinite în ipoteza în care persoana în cauză s-ar fi aflat pe teritoriul statului membru solicitant; și (c) condițiile pentru prelevarea și analizarea materialului biologic, precum și pentru transmiterea profilului ADN obținut sunt reunite, în conformitate cu dreptul statului membru solicitat.		Articolul 12. Prelevarea de material biologic și transmiterea profilurilor ADN (1) În cazul în care, în cadrul unei cauze penale aflate în curs, autoritatea competentă de aplicare a legii a unui stat membru al Uniunii Europene solicită obținerea profilului ADN al unei persoane determinate, iar persoana vizată se află pe teritoriul Republicii Moldova și profilul ADN al acesteia nu este disponibil în Registrul de stat al datelor genetice, autoritățile competente de aplicare a legii ale Republicii Moldova acordă asistență juridică internațională în materie penală, în condițiile prezentei legi și ale legislației naționale aplicabile. (2) Asistența prevăzută la alin. (1) constă, după caz, în: a) dispunerea și efectuarea prelevării materialului biologic al persoanei vizate; b) analizarea materialului biologic și determinarea profilului ADN; c) transmiterea profilului ADN obținut către statul solicitant. (3) Prelevarea materialului biologic se efectuează

			exclusiv în condițiile și cu garanțiile prevăzute de legislația procesual-penală a Republicii Moldova. (4) Cererea se transmite și se execută potrivit normelor privind cooperarea judiciară internațională în materie penală aplicabile, prezenta lege aplicându-se în completare, în măsura compatibilității.
Articolul 8. Date dactiloscopice În vederea aplicării prezentei decizii, statele membre asigură disponibilitatea datelor de referință din fișier pentru sistemele naționale automatizate de identificare a amprentelor create în vederea prevenirii și cercetării infracțiunilor. Datele de referință conțin numai date dactiloscopice și un număr de identificare. Datele de referință nu conțin nicio dată care să permită identificarea directă a persoanei vizate. Datele de referință care nu sunt atribuite niciunei persoane („date dactiloscopice neidentificate”) trebuie să poată fi recunoscute ca atare.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 13. Date dactiloscopice de referință (1) În scopul prevenirii, depistării și investigării infracțiunilor, autoritatea competentă de aplicare a legii, asigură disponibilitatea, pentru efectuarea căutărilor automatizate a datelor dactiloscopice de referință stocate în Registrul de stat dactiloscopic. (2) Datele dactiloscopice de referință utilizate pentru schimbul automatizat de date conțin datele necesare efectuării căutării și nu includ date de identificare directă a persoanei. (3) Datele dactiloscopice neidentificate se marchează

			distinct și sunt recunoscute ca atare în cadrul sistemului de schimb automatizat și al Registrului de stat dactiloscopic.
Articolul 9. Căutarea automatizată a datelor dactiloscopice (1) În vederea prevenirii și cercetării infracțiunilor, statele membre autorizează punctele naționale de contact ale altor state membre, astfel cum sunt menționate la articolul 11, să aibă acces la datele de referință în sistemele automatizate de identificare a amprentelor digitale pe care le-au creat în acest scop, autorizându-le să efectueze căutări automatizate prin compararea datelor dactiloscopice. Căutările pot fi efectuate numai în cazuri individuale și în conformitate cu legislația națională a statului membru solicitant. (2) Stabilirea concordanței datelor dactiloscopice cu date de referință deținute de statul membru care gestionează fișierul se efectuează de punctul național de contact al statului membru solicitant prin intermediul transmiterii automatizate a datelor de referință necesare pentru stabilirea unei concordanțe certe.	<i>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</i> Anexa nr.1 Punctul 63. Căutările automatizate prevăzute în prezenta secțiune se efectuează exclusiv în cadrul unor cazuri individuale și în conformitate cu dreptul intern. Punctul 55. 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. Anexa nr.2 Punctul 43. 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	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 14. Căutarea automatizată a datelor dactiloscopice (1) În scopul prevenirii, depistării și investigării infracțiunilor, autoritatea competentă de aplicare a legii asigură căutarea automatizată în datele dactiloscopice de referință din Registrul de stat dactiloscopic, la solicitarea punctului național de contact al statelor membre ale Uniunii Europene și Europol, în condițiile cadrului normativ în domeniul de cooperare aplicabil. Căutările se realizează prin solicitare automatizată, fără acordarea accesului direct la conținutul Registrului de stat dactiloscopic. (2) Căutările automatizate prevăzute la alin. (1) se efectuează numai în cazuri individuale. În cazul în care autoritatea competentă de aplicare a legii are calitatea

	securitatea interfeței tehnice a sistemelor proprii cu Router-ul UE, facilitând accesul automatizat al partenerilor internaționali, prin intermediul infrastructurii gestionate de PUC.	de solicitant, inițierea și efectuarea căutărilor se realizează în conformitate cu prezenta lege și normele privind protecția datelor cu caracter personal, iar dacă autoritatea competentă de aplicare a legii are calitatea de solicitat, cererile se examinează și se execută în condițiile prezentei legi și ale cadrului normativ național aplicabil. (3) Dacă în urma căutării automatizate autoritatea competentă de aplicare a legii primește un rezultat pozitiv („hit”), confirmarea concordanței dintre seturile de date dactiloscopice se realizează numai după efectuarea unei verificări manuale de cel puțin un membru al personalului calificat, în scopul validării concordanței pe baza datelor dactiloscopice de referință primite. În cazul confirmării concordanței, punctul național de contact informează fără întârziere punctul de contact din statul membru solicitat, potrivit procedurilor stabilite.

Articolul 10. Transmiterea de date suplimentare cu caracter personal și de alte informații În cazul în care procedura menționată la articolul 9 indică o concordanță între datele dactiloscopice, transmiterea de date suplimentare cu caracter personal și de alte informații în legătură cu datele de referință se realizează în temeiul legislației naționale, inclusiv al dispozițiilor privind asistența judiciară, a statului membru solicitat.	<i>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</i> Anexa nr.1 Punctul 76. În cazul în care o căutare automatizată indică o concordanță (hit), PUC recepționează notificarea automatizată conținând datele de referință corespunzătoare. Punctul 77. Orice concordanță identificată este supusă unei revizuii manuale de către cel puțin un membru calificat al personalului, în scopul confirmării validității acesteia pe baza datelor de referință primite. Punctul 78. 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: 78.1. concordanța a fost confirmată manual conform pct. 77; 78.2. a fost transmisă o descriere a faptelor și a fost indicată infracțiunea subiacentă, utilizând tabelul comun al categoriilor de infracțiuni stabilit la nivelul Uniunii Europene, în vederea evaluării proporționalității cererii în conformitate cu legislația națională. Punctul 79. Prin derogare de la pct. 78, termenul poate fi prelungit strict cu o perioadă necesară pentru obținerea unei autorizații judiciare, în cazul în care legislația	Compatibil	

	națională condiționează transmiterea datelor de o astfel de autorizație. Punctul 80. În cazul datelor identificate, datele de bază cuprind, în măsura disponibilității: 80.1. numele, prenumele; 80.2. data nașterii; 80.3. pseudonimele; 80.4. cetățenia; 80.5. locul și țara nașterii; 80.6. genul; 80.7. data și locul obținerii datelor biometrice; 80.8. infracțiunea aferentă; 80.9. numărul cauzei penale; 80.10. autoritatea responsabilă. Punctul 81. 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. Punctul 82. 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.		
Articolul 11. Punctul național de contact și măsurile de punere în aplicare (1) Fiecare stat membru desemnează un punct național de contact în scopul furnizării datelor menționate la articolul 9. Competențele punctelor naționale de contact sunt reglementate de legislația națională aplicabilă. (2) Măsurile de punere în aplicare, astfel cum sunt menționate la articolul 33, stabilesc	<i>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</i> Punctul 1. Se desemnează următoarele autorități în calitate de Puncte Naționale de Contact, pe domenii de competență sau, după caz, pentru asigurarea conectivității tehnice	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 6. Punctul unic de contact și atribuțiile acestuia (1) Se desemnează în calitate de punct unic de contact pentru cooperarea polițienească internațională

detaliile tehnice ale procedurii descrise la articolul 9.	securizate necesare schimbului de date, 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 al MAI – pentru domeniul evidențelor poliției cu caracter criminal, contravențional, datele nominale privind persoanele urmărite, dispărute sau implicate în activități infracționale, 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 al MAI – pentru domeniul evenimentelor majore cu dimensiune transfrontalieră; 1.4. Agencia Servicii Publice – pentru domeniul de date privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, date privind documentele de călătorie, vizele, titlurile de valoare, inclusiv		subdiviziunea specializată în cooperare polițienească internațională din subordinea Inspectoratului General al Poliției al Ministerului Afacerilor Interne. (2) Punctul unic de contact asigură cooperarea cu punctele naționale de contact desemnate prin hotărâre de Guvern, din cadrul autorităților competente naționale, pe următoarele domenii: b) date dactiloscopice; (7) Organizarea, funcțiile și modul de funcționare a punctului unic de contact și a punctelor naționale de contact pe domeniile prevăzute la alin. (2), se stabilesc prin hotărâre de Guvern.

	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 teroriste; 1.6. Serviciul Tehnologia Informației și Securitate Cibernetică – în calitate de punct național de contact tehnic pentru rețeaua securizată S-TESTA, responsabil de asigurarea conectivității, funcționării, disponibilității și securității canalului național de comunicații utilizat pentru schimbul de date. Punctul 2. Se aprobă: 2.1. Regulamentul de organizare și funcționare a Punctului Unic de Contact în scopul schimbului de date și informații, conform anexei nr. 1; 2.2. Regulamentul de organizare și funcționare a Punctelor Naționale de Contact în scopul schimbului de date și informații, conform anexei nr. 2.		
Articolul 12. Căutarea automatizată a datelor privind înmatricularea vehiculelor (1) În vederea prevenirii și cercetării infracțiunilor și în cursul cercetării altor infracțiuni care sunt de competența instanțelor judecătorești sau a parchetelor din statul membru care efectuează căutarea, precum și în cursul menținerii siguranței publice, statele membre autorizează punctele naționale de contact ale altor state membre, astfel cum sunt menționate la alineatul (2), să aibă acces la următoarele date naționale privind înmatricularea vehiculelor, autorizându-le să	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 Anexa nr.1 Punctul 63. Căutările automatizate prevăzute în prezenta secțiune se efectuează exclusiv în cadrul unor cazuri individuale și în conformitate cu dreptul intern. Punctul 74. Căutările automatizate în datele privind mijloacele de transport prin intermediul sistemului EUCARIS pot fi	Compatibil	Proiectul de lege privind cooperarea polițienească internațională Articolul 6. Punctul unic de contact și atribuțiile acestuia (1) Se desemnează în calitate de punct unic de contact pentru cooperarea polițienească internațională subdiviziunea specializată în cooperare polițienească internațională din subordinea

efectueze căutări automatizate în cazuri individuale: (a) datele privind proprietarii sau, după caz, utilizatorii; și (b) datele privind vehiculele. Căutările pot fi efectuate doar prin utilizarea unui număr complet de identificare a vehiculului sau a unui număr complet de înmatriculare. Căutările pot fi efectuate numai în conformitate cu legislația națională a statului membru care efectuează căutarea. (2) Fiecare stat membru desemnează un punct național de contact în scopul furnizării datelor menționate la alineatul (1). Competențele punctelor naționale de contact sunt reglementate de legislația națională aplicabilă. Măsurile de punere în aplicare, astfel cum sunt menționate la articolul 33, stabilesc detaliile tehnice ale procedurii.	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 pentru menținerea siguranței publice. Punctul 75. Categoriile de date accesate prin EUCARIS Schimbul automatizat de date prin interfața EUCARIS permite accesul autorităților competente la următoarele seturi de date de referință din registrele naționale: 75.1. date privind proprietarii sau, după caz, utilizatorii vehiculelor; 75.2. 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. Anexa nr.2 Punctul 62. ASP este desemnată în calitate de PNC responsabil de gestionarea bazelor de date naționale privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, a datelor referitoare la documente de călătorie, vizele, titlurile de valoare, inclusiv a celor declarate false, furate sau pierdute, precum și a datelor		Inspectoratului General al Poliției al Ministerului Afacerilor Interne. (2) Punctul unic de contact asigură cooperarea cu punctele naționale de contact desemnate prin hotărâre de Guvern, din cadrul autorităților competente naționale, pe următoarele domenii: c) date referitoare la mijloace de transport, inclusiv autovehicule anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale;

	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.		
Articolul 13. Transmiterea datelor care nu privesc persoanele În vederea prevenirii infracțiunilor și a menținerii ordinii și siguranței publice în cursul evenimentelor majore care au o dimensiune transfrontalieră, în special în cazul evenimentelor sportive sau al reuniunilor Consiliului European, statele membre își transmit reciproc, atât la cerere, cât și din proprie inițiativă, date care nu privesc persoanele ce pot fi necesare în acest scop, în conformitate cu legislația națională a statului membru care transmite datele.	<i>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</i> Anexa nr.1 Punctul 10. PUC acționează ca interfață unică și centralizată între sistemele informaționale naționale și infrastructura centrală a Uniunii Europene, fiind structura administrativă și operațională desemnată la nivel național pentru a asigura fluxul informațional securizat cu statele membre ale Uniunii Europene, alte state și organizațiile internaționale profilate pe schimbul de date și informații de natură infracțională, având următoarele atribuții funcționale și operaționale principale: 10.1. asigurarea notificării oficiale către Secretariatul General al Consiliului Uniunii Europene și Comisiei Europene, în termen de cel mult o lună de la data desemnării, cu privire la desemnarea PUC și a Punctelor Naționale de Contact (în continuare – PNC) pe domenii de competență, precum și a listei limbilor stabilite pentru schimbul de informații conform pct. 39, inclusiv a	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 6. Punctul unic de contact și atribuțiile acestuia (1) Se desemnează în calitate de punct unic de contact pentru cooperarea polițienească internațională subdiviziunea specializată în cooperare polițienească internațională din subordinea Inspectoratului General al Poliției al Ministerului Afacerilor Interne. (2) Punctul unic de contact asigură cooperarea cu punctele naționale de contact desemnate prin hotărâre de Guvern, din cadrul autorităților competente naționale, pe următoarele domenii: f) date care nu privesc persoanele și informații operative;

	oricăror modificări ulterioare ale acestora, în vederea publicării în Jurnalul Oficial al Uniunii Europene sau pe platformele online dedicate ale Comisiei; 10.2. 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; Anexa nr.2 Punctul 55. IGC al MAI este desemnat în calitate de PNC responsabil pentru domeniul evenimentelor majore cu dimensiune transfrontalieră, având rolul de a furniza și de a schimba informații cu PUC și entitățile similare din statele membre în scopul menținerii ordinii și siguranței publice. Aceste activități vizează prevenirea, depistarea și investigarea infracțiunilor, precum și gestionarea riscurilor asociate evenimentelor cu impact transfrontalier. Punctul 56. 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 din cadrul IGC, care operează prin intermediul canalelor Europol și al mecanismelor europene de cooperare polițienească. Punctul 57. 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.		
Articolul 14. Transmiterea datelor cu caracter personal (1) În vederea prevenirii infracțiunilor și a menținerii ordinii și siguranței publice în cursul evenimentelor majore care au o dimensiune transfrontalieră, în special în cazul evenimentelor sportive sau al reuniunilor Consiliului European, statele membre își transmit reciproc, atât la cerere, cât și din proprie inițiativă, date cu caracter personal, atunci când orice condamnări definitive sau alte împrejurări îndreptățesc convingerea că persoanele vizate vor săvârși infracțiuni cu ocazia evenimentelor sau că acestea prezintă un pericol pentru ordinea și siguranța publică, atât timp cât transmiterea acestor date este permisă în temeiul legislației naționale a statului membru care furnizează datele.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 28. Transmiterea datelor cu caracter personal pentru evenimente majore cu dimensiune transfrontalieră și garanțiile de protecție și securitate (1) În scopul prevenirii infracțiunilor, menținerii ordinii și securității publice în contextul evenimentelor majore cu dimensiune transfrontalieră, autoritățile competente pot transmite și primi, la cerere sau din proprie inițiativă, date cu caracter personal și informații care nu conțin astfel de date către sau de la autoritățile competente ale statelor membre ale Uniunii Europene.

			(2) Transmiterea sau primirea datelor potrivit alin. (1) se efectuează numai dacă este necesară și proporțională în raport cu scopul urmărit și există informații pertinente și verificabile, inclusiv condamnări definitive ori alte date obiective, din care rezultă că persoana vizată ar putea săvârși infracțiuni sau ar putea constitui un risc real pentru ordinea și securitatea publică. Prelucrarea se realizează cu respectarea legislației naționale privind protecția datelor cu caracter personal, a securității informației și a regulilor aplicabile cooperării polițienești internaționale.
(2) Datele cu caracter personal pot fi prelucrate numai în scopurile prevăzute la alineatul (1) și pentru evenimentele concrete pentru care acestea au fost furnizate. Din momentul în care obiectivele prevăzute la alineatul (1) au fost sau nu mai pot fi atinse, datele transmise trebuie șterse fără întârziere. În orice situație, datele transmise trebuie șterse după cel mult un an.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 28. Transmiterea datelor cu caracter personal pentru evenimente majore cu dimensiune transfrontalieră și garanțiile de protecție și securitate (3) Datele cu caracter personal primite sau transmise în temeiul prezentului articol se șterg cel târziu la expirarea termenului de 1 an de la data furnizării, cu excepția cazului

			în care există un temei legal pentru păstrarea lor pentru o perioadă mai mare, în cadrul unei proceduri legale distincte. (4) Autoritatea competentă de aplicare a legii desemnează un punct național de contact responsabil pentru schimbul de date privind transmiterea informațiilor în contextul evenimentelor majore cu dimensiune transfrontalieră, iar atribuțiile, organizarea și modul de funcționare ale acestuia se stabilesc de Guvern.
Articolul 15. Punctul național de contact Fiecare stat membru desemnează un punct național de contact în scopul furnizării datelor menționate la articolele 13 și 14. Competențele punctelor naționale de contact sunt reglementate de legislația națională aplicabilă.	<i>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</i> Anexa nr.2 Punctul 55. IGC al MAI este desemnat în calitate de PNC responsabil pentru domeniul evenimentelor majore cu dimensiune transfrontalieră, având rolul de a furniza și de a schimba informații cu PUC și entitățile similare din statele membre în scopul menținerii ordinii și siguranței publice. Aceste activități vizează prevenirea, depistarea și investigarea infracțiunilor, precum și gestionarea riscurilor asociate evenimentelor cu impact transfrontalier.	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 6. Punctul unic de contact și atribuțiile acestuia (1) Se desemnează în calitate de punct unic de contact pentru cooperarea polițienească internațională subdiviziunea specializată în cooperare polițienească internațională din subordinea Inspectoratului General al Poliției al Ministerului Afacerilor Interne. (2) Punctul unic de contact asigură cooperarea cu punctele naționale de contact

	Punctul 56. 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 din cadrul IGC, care operează prin intermediul canalelor Europol și al mecanismelor europene de cooperare polițienească. Punctul 57. 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.		desemnate prin hotărâre de Guvern, din cadrul autorităților competente naționale, pe următoarele domenii: f) date care nu privesc persoanele și informații operative; g) date cu caracter personal prelucrate în contextul evenimentelor majore cu dimensiune transfrontalieră și de prevenire a infracțiunilor cu caracter terorist;
Articolul 16 Transmiterea informațiilor în vederea prevenirii infracțiunilor teroriste (1) În vederea prevenirii infracțiunilor teroriste, în conformitate cu legislația națională și, în cazuri individuale, chiar fără a fi solicitate, statele membre pot furniza punctelor naționale de contact ale altor state membre, astfel cum se menționează la alineatul (3), datele cu caracter personal și informațiile prevăzute la alineatul (2), în măsura în care acest lucru se dovedește necesar pentru că împrejurări determinate îndreptățesc convingerea că persoanele vizate vor săvârși		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 29. Transmiterea informațiilor în vederea prevenirii infracțiunilor cu caracter terorist (1) Autoritatea competentă de aplicare a legii poate transmite, în conformitate cu legislația națională și în cazuri individuale, inclusiv din

infrațiuni precum cele menționate la articolele 1-3 din Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului.			proprie inițiativă, punctelor naționale de contact ale altor state, date cu caracter personal și informații necesare prevenirii infracțiunilor cu caracter terorist, atunci când circumstanțele justifică în mod rezonabil concluzia că persoanele vizate pot săvârși infracțiuni cu caracter terorist pe teritoriul statului respectiv.
(2) Datele care urmează a fi transmise conțin numele, prenumele, data și locul nașterii, precum și o descriere a împrejurărilor care conduc la convingerea menționată la alineatul (1).		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 29. Transmiterea informațiilor în vederea prevenirii infracțiunilor cu caracter terorist (2) Datele cu caracter personal transmise în acest scop includ: a) numele și prenumele persoanei vizate; b) data și locul nașterii; c) o descriere a împrejurărilor specifice din care rezultă o bănuială rezonabilă că persoana respectivă urmează să săvârșească infracțiuni cu caracter terorist.
(3) Fiecare stat membru desemnează un punct național de contact în vederea schimbului de informații cu punctele naționale de contact ale altor state membre.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i>

Competențele punctelor naționale de contact sunt reglementate de legislația națională aplicabilă.			Articolul 29. Transmiterea informațiilor în vederea prevenirii infracțiunilor cu caracter terorist (3) Autoritatea competentă de aplicare a legii desemnează un punct național de contact pentru realizarea schimbului de informații prevăzut la prezentul articol. Atribuțiile, competențele și modalitatea de funcționare a acestuia se stabilesc de Guvern
(4) Statul membru care transmite datele poate stabili, în conformitate cu legislația națională, condițiile privind utilizarea unor asemenea date și informații de către statul membru destinatar. Statul membru destinatar este obligat să respecte aceste condiții.		Compatibil	Proiectul de lege privind cooperarea polițienească internațională Articolul 29. Transmiterea informațiilor în vederea prevenirii infracțiunilor cu caracter terorist (4) Autoritatea competentă de aplicare a legii care transmite date poate stabili condiții referitoare la utilizarea exclusivă a datelor de către statul destinatar, iar destinatarul este obligat să respecte condițiile stabilite.
Articolul 17. Operațiuni comune (1) În vederea intensificării cooperării polițienești, în cursul menținerii ordinii și securității publice și al prevenirii infracțiunilor, autoritățile competente		Compatibil	Proiectul de lege privind cooperarea polițienească internațională Articolul 30. Organizarea patrulilor și

desemnate de statele membre pot forma patrulare comune și desfășura alte operațiuni comune, în care agenți desemnați sau alți oficiali (denumiți în continuare „agenți”) din alte state membre participă la operațiuni pe teritoriul altui stat membru.			operațiunilor comune pe teritoriul Republicii Moldova (1) Autoritățile competente pot participa, în condițiile prezentei legi, ale legislației naționale aplicabile și ale tratatelor internaționale sau aranjamentelor de cooperare aplicabile, la constituirea de patrulare comune și la desfășurarea operațiunilor comune cu autoritățile competente ale altor state, în scopul menținerii ordinii și securității publice, prevenirii, descoperirii și combaterii infracțiunilor.
(2) În calitate de stat gazdă și în conformitate cu legislația sa națională și cu consimțământul statului membru care a dispus detașarea, fiecare stat membru poate conferi competente de executare agenților statului membru care a dispus detașarea implicați în operațiuni comune sau, în măsura în care legea statului gazdă permite acest lucru, poate permite agenților statelor membre care au dispus detașarea să își exercite propriile competente de executare, în conformitate cu legislația statului membru care a dispus detașarea. Asemenea competențe de executare pot fi exercitate doar sub îndrumarea și, de regulă, în prezența agenților statului gazdă. Agenții statelor membre care au dispus detașarea se supun legislației naționale a statului membru gazdă. Statul membru gazdă		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 30. Organizarea patrulilor și operațiunilor comune pe teritoriul Republicii Moldova (2) Pe teritoriul Republicii Moldova, participarea personalului autorităților străine la astfel de operațiuni se realizează cu acordul autorităților naționale competente. Exercitarea competențelor de către acest personal este permisă numai în condițiile și limitele stabilite de legislația

își asumă răspunderea pentru acțiunile acestora.			Republicii Moldova, sub coordonarea și în prezența personalului autorităților naționale. Personalul străin este supus legislației Republicii Moldova pe durata desfășurării operațiunilor, iar autoritățile naționale asigură coordonarea și controlul activităților desfășurate pe teritoriul statului.
(3) Agenții statelor membre care au dispus detașarea care sunt implicați în operațiuni comune se supun instrucțiunilor date de autoritatea competentă a statului membru gazdă.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 30. Organizarea patrulilor și operațiunilor comune pe teritoriul Republicii Moldova (3) Personalul autorităților competente ale Republicii Moldova care participă la operațiuni comune pe teritoriul altui stat acționează în conformitate cu instrucțiunile autorităților competente ale statului gazdă, fiind supus obligațiilor de serviciu și regimului disciplinar potrivit legislației Republicii Moldova, în măsura în care acestea nu contravin dispozițiilor obligatorii ale statului gazdă.
(4) Statele membre prezintă declarații, astfel cum se menționează la articolul 36, în care stabilesc aspectele practice ale cooperării.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i>

			Articolul 30. Organizarea patrurilor și operațiunilor comune pe teritoriul Republicii Moldova (4) Înainte de începerea unei patrule sau a unei operațiuni comune specifice pe teritoriul Republicii Moldova, autoritățile competente naționale și autoritățile competente ale celorlalte state membre stabilesc printr-un document de cooperare: a) autoritățile competente participante; b) scopul specific al patrului sau operațiunii comune; c) zona geografică a statului în care se desfășoară patrula sau operațiunea comună; d) perioada în care se derulează patrula sau operațiunea comună; e) asistența specifică ce urmează să fie furnizată Republicii Moldova de către statul membru, inclusiv în ceea ce privește trimiterea de personal, elementele materiale și financiare; f) personalul care participă la patrula sau operațiunea comună;

			g) conducătorul echipei comune; h) atribuțiile pe care le pot exercita personalul autorităților competente ale celorlalte state membre pe teritoriul Republicii Moldova în timpul patrului sau operațiunii comune; i) armamentul, muniția și echipamentele specifice pe care personalul autorităților competente ale celorlalte state membre le pot utiliza în timpul patrului sau operațiunii comune; j) modalitățile logistice privind transportul, cazarea și securitatea; k) modul de alocare a costurilor patrului sau operațiunii comune; l) orice alte elemente necesare. (5) Aspectele practice privind organizarea, coordonarea și desfășurarea operațiunilor comune se stabilesc prin declarații, acorduri sau aranjamente administrative care nu sunt guvernate de normele dreptului internațional public, încheiate între autoritățile competente, care nu pot deroga de la limitele

			competențelor stabilite prin lege.
Articolul 18. Asistența în cazul unor reuniuni de masă, dezastre și accidente grave Autoritățile competente din statele membre își oferă asistență reciprocă, în conformitate cu legislația națională, în cazul unor reuniuni de masă, dezastre și în cazul altor evenimente majore, precum și în cazul unor accidente grave, urmărind să prevină infracțiunile și să mențină ordinea și siguranța publică prin: (a) notificarea reciprocă și cât mai promptă a unor asemenea situații cu impact transfrontalier, precum și prin schimbul oricăror informații relevante; (b) adoptarea și coordonarea măsurilor de poliție necesare pe propriul teritoriu în situațiile cu impact transfrontalier; (c) pe cât posibil, detașarea de agenți, specialiști și consilieri și punerea la dispoziție de echipament, la cererea statului membru pe al cărui teritoriu a apărut situația respectivă.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 33. Asistența în cazul evenimentelor transfrontaliere, dezastrelor și accidentelor grave (1) Autoritățile competente de aplicare a legii ale Republicii Moldova acordă, în condiții de reciprocitate și în conformitate cu legislația națională, asistență autorităților similare din statele membre în cazul: a) evenimentelor majore cu dimensiune transfrontalieră; b) dezastrelor; c) accidentelor grave de transport rutier, aviatic sau feroviar; d) altor situații de urgență care necesită cooperare operativă. (2) Asistența reciprocă prevăzută la alin. (1) are ca scop prevenirea infracțiunilor, menținerea ordinii și siguranței publice, realizându-se prin următoarele modalități:

			a) notificarea reciprocă, despre apariția unor astfel de situații și schimbul operativ de informații relevante; b) adoptarea și coordonarea măsurilor polițienești și ale carabinierilor, necesare pe propriul teritoriu, pentru gestionarea situațiilor cu impact transfrontalier; c) detașarea de personal, specialiști și consilieri, precum și punerea la dispoziție de echipament tehnic, la solicitarea statului pe al cărui teritoriu a survenit situația respectivă, în măsura posibil (3) Înainte de acordarea asistenței potrivit dispozițiilor alin. (1) pe teritoriul statului membru, autoritățile competente de aplicare a legii ale Republicii Moldova și autoritățile competente ale celorlalte state stabilesc de comun acord elementele stipulate la art. 32 alin. (2).
Articolul 19. Folosirea armamentului, a munițiilor și a echipamentelor (1) Agenții dintr-un stat membru care a dispus detașarea care participă la o operațiune comună pe teritoriul unui alt stat membru în conformitate cu articolul 17 sau 18 își pot purta uniforme naționale pe teritoriul aceluia stat.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 40. Utilizarea armamentului, a munițiilor și a echipamentelor

Agenții pot avea asupra lor armamentul, muniția și echipamentele care le sunt permise în conformitate cu legislația națională a statului membru care a dispus detașarea. Statul membru gazdă poate interzice portul anumitor arme, muniții sau echipamente de către agenții unui stat membru care a dispus detașarea.			(1) Personalul autorităților competente ale unui stat membru participant, detașat și implicat în operațiuni comune pe teritoriul Republicii Moldova, poate purta uniforme naționale și poate avea asupra lor armament, muniție și echipamente permise de legislația națională, în măsura în care portul, deținerea și utilizarea acestora sunt permise. Autoritățile competente ale Republicii Moldova pot interzice portul armamentului, munițiilor sau echipamentelor de către personalul statului participant.
(2) Statele membre prezintă declarațiile prevăzute la articolul 36 în care enumeră armele, muniția și echipamentele care pot fi folosite doar în legitimă apărare sau pentru apărarea altor persoane. Agentul statului membru gazdă care se află la comanda efectivă a operațiunii poate permite, în anumite cazuri și în conformitate cu legislația națională, folosirea armamentului, a muniției și a echipamentelor și în alte scopuri decât cele prevăzute la prima teză. Folosirea armelor, a muniției și a echipamentelor este reglementată de legislația statului gazdă. Autoritățile competente se informează reciproc cu privire la armamentul, muniția și echipamentele		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 40. Utilizarea armamentului, a munițiilor și a echipamentelor (2) Republica Moldova și statele participante notifică reciproc lista armelor, munițiilor și echipamentelor a căror utilizare este permisă exclusiv în scopul legitim al apărării sau pentru apărarea altor persoane. În cazuri justificate și cu respectarea legislației

permise și cu privire la condițiile în care pot fi folosite.			Republicii Moldova, conducătorul operațiunii aflat sub comanda efectivă a autorităților competente de aplicare a legii poate autoriza folosirea armamentului, a munițiilor și a echipamentelor și în alte scopuri decât cele prevăzute în prezentul alineat. (3) Folosirea armelor, munițiilor și echipamentelor pe teritoriul Republicii Moldova se realizează în conformitate cu legislația națională, iar autoritățile competente de aplicare a legii se informează reciproc cu privire la tipurile de armament, muniții și echipamente permise, precum și la condițiile de port și de utilizare a acestora.
(3) În cazul în care agenții dintr-un stat membru folosesc, într-o acțiune întreprinsă în conformitate cu prezenta decizie, vehicule pe teritoriul unui alt stat membru, aceștia se supun aceluiași reguli privind traficul rutier care se aplică și agenților statului membru gazdă, inclusiv în ceea ce privește dreptul la liberă trecere și orice privilegii speciale.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 40. Utilizarea armamentului, a munițiilor și a echipamentelor (4) În cazul în care personalul statelor participante utilizează vehicule pe teritoriul Republicii Moldova în cadrul unei acțiuni desfășurate potrivit prezentei legi, aceștia se supun regulilor naționale

			privind circulația rutieră, inclusiv în ceea ce privește dreptul de prioritate și eventualele regimuri speciale, în condițiile legii.
(4) Statele membre prezintă declarațiile menționate la articolul 36, în care stabilesc aspectele practice ale folosirii armamentului, a muniției și a echipamentelor.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 40. Utilizarea armamentului, a munițiilor și a echipamentelor (5) Republica Moldova include în declarațiile și notificările privind operațiunile comune aspectele practice referitoare la portul, folosirea și controlul armamentului, munițiilor și echipamentelor. Procedura de elaborare, actualizare și aplicare a acestor declarații sau notificări se stabilește prin aranjamentele de implementare convenite între autoritățile competente.
Articolul 20. Protecția și asistența Statele membre trebuie să ofere agenților altor state membre care traversează frontiera, în exercitarea atribuțiilor de serviciu, aceeași protecție și asistență ca și propriilor lor agenți.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 40. Utilizarea armamentului, a munițiilor și a echipamentelor (6) Republica Moldova asigură personalului autorităților competente de aplicare a legii ale statelor participante care traversează

			frontiera de stat sau se află pe teritoriul său, în exercitarea atribuțiilor de serviciu în cadrul cooperării transfrontaliere, aceeași protecție juridică, operativă și aceeași asistență ca și personalului autorităților competente naționale, în condițiile legislației naționale.
Articolul 21. Regulile generale cu privire la răspunderea civilă (1) Atunci când agenți ai unui stat membru desfășoară operațiuni într-un alt stat membru în conformitate cu articolul 17, statul membru din care provin răspunde pentru orice prejudicii cauzate de aceștia în cursul operațiunilor lor, în conformitate cu legislația statului membru pe teritoriul căruia își desfășoară operațiunile.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 41. Regulile generale privind răspunderea civilă, penală și a raporturilor de muncă (1) În cazul în care personalul autorităților competente ale unui stat membru desfășoară operațiuni pe teritoriul Republicii Moldova, în cadrul cooperării internaționale prevăzute de prezenta lege, statul membru de origine răspunde pentru prejudiciile cauzate de personalul său, în conformitate cu legislația sa.
(2) Statul membru pe al cărei teritoriu s-au produs prejudiciile menționate la alineatul (1) repară aceste prejudicii în condițiile aplicabile prejudiciilor cauzate de proprii săi agenți.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 41. Regulile generale privind răspunderea civilă, penală și a raporturilor de muncă

			(2) Republica Moldova repară prejudiciile prevăzute la alin. (1) în aceleași condiții aplicabile prejudiciilor cauzate de propriul său personal, potrivit legislației naționale.
(3) În cazul menționat la alineatul (1), statul membru ai cărui agenți au cauzat prejudicii unei persoane de pe teritoriul unui alt stat membru rambursează acestuia din urmă totalitatea sumelor pe care le-a plătit victimelor sau persoanelor îndreptățite în numele acestora.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 41. Regulile generale privind răspunderea civilă, penală și a raporturilor de muncă (3) Statul membru al cărui personal a cauzat prejudiciul rambursează Republicii Moldova integral sumele plătite victimelor sau persoanelor îndreptățite, după caz.
(4) Atunci când agenți ai unui stat membru desfășoară operațiuni într-un alt stat membru conform articolului 18, statul membru gazdă răspunde pentru orice prejudicii cauzate de aceștia în cursul operațiunilor lor, în conformitate cu legislația sa națională.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 41. Regulile generale privind răspunderea civilă, penală și a raporturilor de muncă (4) În cazul în care personalul unui stat membru participant desfășoară operațiuni pe teritoriul Republicii Moldova ca parte a asistenței acordate la solicitarea autorităților naționale, Republica Moldova

			răspunde pentru prejudiciile cauzate de acesta, în conformitate cu legislația sa națională.
(5) Atunci când prejudiciile menționate la alineatul (4) s-au produs ca urmare a unei fapte săvârșite din culpă gravă sau cu intenție, statul membru gazdă poate solicita statului membru care a dispus detașarea rambursarea oricăror sume pe care le-a plătit victimelor sau persoanelor îndreptățite a fi despăgubite în numele acestora.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 41. Regulile generale privind răspunderea civilă, penală și a raporturilor de muncă (5) Dacă prejudiciile prevăzute la alin. (4) au fost cauzate intenționat, Republica Moldova poate solicita statului participant care a dispus detașarea, rambursarea sumelor plătite victimelor sau persoanelor îndreptățite.
(6) Fără a aduce atingere exercitării drepturilor sale față de terțe părți și cu excepția alineatului (3), fiecare stat membru se abține în cazul prevăzut la alineatul (1) de a pretinde de la un alt stat membru rambursarea despăgubirilor pentru prejudiciile suferite.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 41. Regulile generale privind răspunderea civilă, penală și a raporturilor de muncă (6) Fără a aduce atingere drepturilor față de terți și cu excepția situației prevăzute la alin. (3), în cazul prevăzut la alin. (1), Republica Moldova se abține de a solicita unui stat participant rambursarea despăgubirilor pentru prejudiciile suferite.

Articolul 22. Răspunderea penală Agenților care acționează pe teritoriul altui stat membru în conformitate cu prezenta decizie li se aplică același tratament ca și celor care aparțin statului membru gazdă în ceea ce privește orice infracțiuni care ar putea fi săvârșite de aceștia sau care ar putea fi săvârșite împotriva lor, cu excepția cazului în care se prevede altfel într-un alt acord cu caracter obligatoriu pentru statele membre în cauză.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 41. Regulile generale privind răspunderea civilă, penală și a raporturilor de muncă (7) Personalul autorităților competente ale statelor membre care acționează pe teritoriul Republicii Moldova în cadrul cooperării transfrontaliere se supune aceluiași regim de răspundere penală și beneficiază de aceeași protecție ca și personalul autorităților competente ale Republicii Moldova, pentru infracțiunile săvârșite de aceștia sau împotriva lor, în conformitate cu legislația Republicii Moldova, cu excepția cazului în care un tratat internațional sau un alt acord internațional cu caracter obligatoriu, la care Republica Moldova este parte, prevede altfel.
Articolul 23. Raporturile de muncă Agenții care acționează pe teritoriul altui stat membru, în conformitate cu prezenta decizie, rămân supuși dispozițiilor din legislația muncii aplicabile în propriul lor stat membru, în special în ceea ce privește normele de disciplină.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 41. Regulile generale privind răspunderea civilă, penală și a raporturilor de muncă

			(8) Personalul autorităților competente ale statelor membre care acționează pe teritoriul Republicii Moldova, rămâne supus dispozițiilor aplicabile raporturilor de muncă din statul care a dispus detașarea, inclusiv normelor privind disciplina în serviciu, fără a aduce atingere respectării legislației Republicii Moldova aplicabile desfășurării activităților pe teritoriul său.
Articolul 24. Definiții și domeniu de aplicare (1) În înțelesul prezentei decizii: (a) „prelucrarea datelor cu caracter personal” înseamnă orice operațiune sau set de operațiuni care sunt efectuate cu privire la datele cu caracter personal, indiferent dacă se realizează sau nu prin mijloace automatizate, precum culegerea, înregistrarea, organizarea, stocarea, adaptarea sau modificarea, sortarea, recuperarea, consultarea, utilizarea, divulgarea prin furnizare, diseminarea sau punerea la dispoziție în alt mod, alinierea, combinarea, blocarea, ștergerea sau distrugerea datelor. Prelucrarea, în sensul prezentei decizii, include comunicarea, indiferent dacă există sau nu „hit” (răspuns pozitiv);		Compatibil	<i>Legea nr. 195/2024 privind protecția datelor cu caracter personal</i> Articolul 4. Noțiuni <i>prelucrare</i> – orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea,

			restricționarea, ștergerea sau distrugerea; <i>date cu caracter personal</i> – orice informații privind o persoană fizică identificată sau identificabilă (în continuare – persoană vizată). Persoana fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special, prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul ori mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;
(b) „procedura de căutare automatizată” înseamnă accesul direct la bazele de date automatizate ale altui organism, în cazul în care răspunsul în urma procedurii de căutare este complet automatizat;		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 3. Noțiuni generale <i>procedura de căutare automatizată</i> – modalitatea tehnică de acces direct și simultan la bazele de date naționale sau internaționale, care permite autorităților competente să verifice existența unei concordanțe (hit) printr-o interogare

			informatică, oferind un răspuns imediat de tip „pozitiv/negativ” (hit/no-hit);
(c) „catalogare” înseamnă marcarea datelor cu caracter personal stocate, fără a avea ca scop limitarea prelucrării lor ulterioare;		Incompatibil	Termenul de „ <i>catalogare</i> ” nu a fost preluat distinct, pentru a evita confuzia cu noțiunea de „marcare a datelor”, care în prezentul proiect de Hotărâre de Guvern are un sens specific și divergent față de cel din Decizia 2008/615/JAI. În proiectul național, „marcarea” este utilizată exclusiv ca măsură de protecție pentru limitarea prelucrării datelor contestate. Funcția tehnică de „catalogare” (pregătirea datelor pentru schimb fără a le limita prelucrarea) este absorbită de procedurile operaționale de administrare a registrelor naționale de către Punctele Naționale de Contact.
(d) „blocare” înseamnă marcarea datelor cu caracter personal stocate, cu scopul de a limita prelucrarea lor ulterioară.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 3. Noțiuni generale <i>blocare de date</i> – marcarea prin acoperire a datelor cu caracter personal stocate, cu scopul de a limita prelucrarea lor ulterioară;

(2) Următoarele dispoziții se aplică datelor care sunt sau au fost furnizate în conformitate cu prezenta decizie, cu excepția cazului în care se prevede altfel în capitolele anterioare.		Prevedere UE neaplicabilă	Prevederea are caracter general și introductiv, stabilind domeniul de aplicare al normelor privind prelucrarea datelor furnizate în temeiul deciziei. Aceasta nu instituie obligații normative autonome care să necesite transpunere distinctă în proiectul de PHG.
Articolul 25. Nivelul de protecție a datelor (1) În privința prelucrării datelor cu caracter personal, care sunt sau au fost furnizate conform prezentei decizii, fiecare stat membru garantează un nivel de protecție a datelor cu caracter personal în legislația sa națională, cel puțin egal cu cel rezultat din Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal din 28 ianuarie 1981 și din Protocolul său adițional din 8 noiembrie 2001, luând astfel în considerare Recomandarea nr. R (87) 15 din 17 septembrie 1987 a Comitetului de Miniștri al Consiliului Europei către statele membre care reglementează utilizarea datelor cu caracter personal în domeniul polițienesc, chiar și în cazul în care datele nu sunt prelucrate automatizat.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 46. Protecția și scopul prelucrărilor datelor cu caracter personal (1) Autoritățile competente asigură protecția datelor cu caracter personal potrivit standardelor stabilite de Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal și Protocolul adițional la Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor, precum și cu principiile aplicabile prelucrării datelor cu caracter personal în domeniul polițienesc, inclusiv

			în cazul în care datele nu sunt prelucrate automatizat.
(2) Transmiterea datelor cu caracter personal reglementată de prezenta decizie nu poate avea loc decât după ce dispozițiile prezentului capitol au fost puse în aplicare în legislația națională aplicabilă pe teritoriile statelor membre implicate în această transmitere. Consiliul decide în unanimitate dacă această condiție a fost îndeplinită.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 46. Protecția și scopul prelucrărilor datelor cu caracter personal (2) Schimbul de date cu statele membre ale Uniunii Europene se realizează în condițiile stabilite prin instrumentele de cooperare aplicabile și după asigurarea funcționalității mecanismelor de protecție a datelor prevăzute de prezenta lege.
(3) Alineatul (2) nu se aplică acelor state membre în care transmiterea de date cu caracter personal reglementată de prezenta decizie a început deja ca urmare a Tratatului de la Prüm din 27 mai 2005 încheiat între Regatul Belgiei, Republica Federală Germania, Regatul Spaniei, Republica Franceză, Marele Ducat al Luxemburgului, Regatul Țărilor de Jos și Republica Austria privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului, a criminalității transfrontaliere și a migrației ilegale („Tratatul de la Prüm”).		Prevedere UE neaplicabilă	Norma vizează exclusiv state membre UE părți la Tratatul de la Prüm și reglementează continuitatea unui regim de cooperare deja existent între acestea.
Articolul 26. Scopul (1) Prelucrarea datelor cu caracter personal de către statul membru destinat este permisă doar pentru scopul pentru care au fost furnizate, în conformitate cu prezenta decizie. Prelucrarea în alt scop este permisă numai cu		Prevedere UE netranspusă	<i>Articolul 46 din proiectul de lege privind cooperarea polițienească internațională</i>, respectiv art. 50 din Regulamentul (UE) 2024/982 preia și dezvoltă

autorizarea prealabilă a statului membru care administrează fișierul și doar cu respectarea legislației naționale a statului membru destinatar. O astfel de autorizație poate fi acordată cu condiția ca prelucrarea în alte scopuri să fie permisă de legislația națională a statului membru care administrează fișierul.			integral regulile din art. 26 al Deciziei 2008/615/JAI privind limitarea scopului, autorizarea prelucrării pentru alte scopuri, utilizările permise după căutări/comparări și obligația de ștergere imediată după răspunsurile automatizate; prin urmare, transpunerea art. 50 asigură acoperirea completă a art. 26 din Decizie.
(2) Prelucrarea datelor furnizate conform articolelor 3, 4 și 9 de către statul membru care efectuează căutarea sau compararea este permisă doar pentru:		Prevedere UE netranspusă	Articolul 46 din proiectul de lege privind cooperarea polițienească internațională, respectiv art. 50 din Regulamentul (UE) 2024/982 preia și dezvoltă integral regulile din art. 26 al Deciziei 2008/615/JAI privind limitarea scopului, autorizarea prelucrării pentru alte scopuri, utilizările permise după căutări/comparări și obligația de ștergere imediată după răspunsurile automatizate; prin urmare, transpunerea art. 50 asigură acoperirea completă a art. 26 din Decizie.
Statul membru care administrează fișierul poate prelucra datele furnizate în conformitate cu articolele 3, 4 și 9 numai atunci când este necesar în scopul comparării, al furnizării răspunsurilor automatizate la căutări sau al înregistrării în conformitate cu articolul 30.		Prevedere UE netranspusă	Articolul 46 din proiectul de lege privind cooperarea polițienească internațională, respectiv art. 50 din Regulamentul (UE) 2024/982 preia și dezvoltă

Datele furnizate sunt șterse îndată după compararea datelor sau după răspunsurile automatizate la căutări, în afara cazului în care este necesară continuarea prelucrării datelor în scopurile menționate la literele (b) și (c) din primul paragraf.			integral regulile din art. 26 al Deciziei 2008/615/JAI privind limitarea scopului, autorizarea prelucrării pentru alte scopuri, utilizările permise după căutări/comparări și obligația de ștergere imediată după răspunsurile automatizate; prin urmare, transpunerea art. 50 asigură acoperirea completă a art. 26 din Decizie.
(3) Datele furnizate în conformitate cu articolul 12 pot fi utilizate de către statul membru care administrează fișierul numai atunci când acest lucru este necesar în scopul furnizării răspunsurilor automatizate la procedurile de căutare sau al înregistrării în conformitate cu articolul 30. Datele furnizate sunt șterse îndată după transmiterea răspunsurilor automatizate la căutări, în afara cazului în care este necesară continuarea prelucrării în vederea înregistrării în conformitate cu articolul 30. Statul membru care efectuează căutarea poate folosi datele primite ca răspuns numai pentru procedura pentru care a fost efectuată căutarea.		Prevedere UE netranspusă	Articolul 46 din proiectul de lege privind cooperarea polițienească internațională, respectiv art. 50 din Regulamentul (UE) 2024/982 preia și dezvoltă integral regulile din art. 26 al Deciziei 2008/615/JAI privind limitarea scopului, autorizarea prelucrării pentru alte scopuri, utilizările permise după căutări/comparări și obligația de ștergere imediată după răspunsurile automatizate; prin urmare, transpunerea art. 50 asigură acoperirea completă a art. 26 din Decizie.
Articolul 27. Autoritățile competente Datele cu caracter personal furnizate pot fi prelucrate doar de către autoritățile, organismele și instanțele cu atribuții care servesc realizării scopurilor prevăzute la articolul 26. În special, datele pot fi furnizate		Compatibil	Proiectul de lege privind cooperarea polițienească internațională Articolul 46. Protecția și scopul prelucrărilor datelor cu caracter personal

altor entități doar cu autorizarea prealabilă din partea statului membru furnizor și în conformitate cu legislația statului membru destinatar.			(1) Autoritățile competente asigură protecția datelor cu caracter personal potrivit standardelor stabilite de Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal și Protocolul adițional la Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor, precum și cu principiile aplicabile prelucrării datelor cu caracter personal în domeniul polițienesc, inclusiv în cazul în care datele nu sunt prelucrate automatizat. (2) Schimbul de date cu statele membre ale Uniunii Europene se realizează în condițiile stabilite prin actele normative de cooperare aplicabile și după asigurarea funcționalității mecanismelor de protecție a datelor prevăzute de prezenta lege. (3) Prelucrarea datelor în alte scopuri decât cele prevăzute de prezenta lege se admite numai cu autorizarea prealabilă a statului

			participant sau a Europol (după caz), precum și în condițiile expres prevăzute de legislația națională. (4) Prelucrarea datelor furnizate de către statele membre ale Uniunii Europene sau de către Europol autorităților competente este permisă exclusiv dacă este necesară pentru: a) stabilirea existenței unei concordanțe între profilurile ADN, datele dactiloscopice, datele privind înmatricularea vehiculelor, imaginile faciale sau evidențele poliției comparate; b) efectuarea schimbului setului de date de bază în urma unei concordanțe confirmate; c) pregătirea și depunerea unei cereri de către organele de drept sau judiciare în vederea acordării de asistență juridică, în cazul obținerii unei concordanțe; d) păstrarea înregistrărilor (log-urilor) necesare pentru monitorizarea legalității și securității datelor
Articolul 28. Acuratețea, relevanța actuală și perioada de stocare a datelor	<i>Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de</i>	Compatibil	

(1) Statele membre asigură acuratețea și relevanța actuală a datelor cu caracter personal. Dacă ex officio sau dintr-o notificare a persoanei vizate rezultă că au fost furnizate date incorecte sau date care nu ar fi trebuit să fie furnizate, acest fapt este notificat de îndată statului sau statelor membre destinate. Statul sau statele membre în cauză sunt obligate să corecteze sau să ștergă datele. De asemenea, datele cu caracter personal furnizate sunt corectate dacă se descoperă că sunt incorecte. Dacă organismul destinatar are motive să creadă că datele furnizate sunt incorecte sau ar trebui șterse, autoritatea care le-a furnizat este informată de îndată despre aceasta.	Contact în scopul schimbului de date și informații Anexa nr.1 Punctul 96. În cazul constatării furnizării unor date incorecte, neactuale sau care nu ar fi trebuit furnizate, PUC notifică imediat autoritatea destinatară, asigurând corectarea sau ștergerea acestora fără întârzieri nejustificate. Punctul 99. 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. Anexa nr.2 Punctul 8. PNC își desfășoară activitatea în baza următoarelor principii specifice prelucrării datelor biometrice și alfanumerice: 8.1. <i>principiul exactității și actualizării</i> — asigurarea caracterului veridic al datelor din registrele naționale și rectificarea sau ștergerea imediată a informațiilor incorecte; Punctul 28. PNC asigură exactitatea și relevanța datelor cu caracter personal prelucrate.		
(2) Datele a căror acuratețe este contestată de persoana vizată sau a căror acuratețe sau lipsă de acuratețe nu poate fi stabilită trebuie să fie marcate cu un steguleț la cererea persoanei vizate, în conformitate cu legislația națională a statelor membre. Dacă există un steguleț, acesta poate fi înlăturat în	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 Anexa nr.2	Compatibil	

conformitate cu legislația națională a statelor membre și numai cu permisiunea persoanei vizate sau pe baza unei hotărâri a instanței judecătorești competente sau a autorității independente de protecție a datelor.	Punctul 29. Dacă o persoană vizată contestă exactitatea datelor deținute de un PNC, iar aceasta nu poate fi stabilită imediat, PNC-ul aplică un indicator de marcare (marcaj) asupra datelor respective. Punctul 30. Marcajul limitează utilizarea datelor până la clarificarea situației și poate fi eliminat doar: 30.1. cu acordul expres al persoanei vizate; 30.2. în baza unei decizii definitive a instanței de judecată; 30.3. în baza unei decizii a Centrului Național pentru Protecția Datelor cu Caracter Personal.		
(3) Datele cu caracter personal furnizate care nu ar fi trebuit furnizate sau primite se șterg. Datele care sunt legal furnizate și primite se șterg: (a) dacă nu sunt sau nu mai sunt necesare pentru scopul pentru care au fost furnizate; dacă datele cu caracter personal au fost furnizate fără a fi solicitate, organismul destinatar verifică de îndată dacă sunt necesare în scopul pentru care au fost furnizate; (b) după expirarea termenului maxim de păstrare a datelor prevăzut de legislația națională a statului membru care furnizează datele, atunci când organismul care a furnizat datele a informat organismul destinatar cu privire la acel termen maxim la momentul furnizării datelor. Atunci când există motive să se creadă că ștergerea ar prejudicia interesele persoanei vizate, datele sunt blocate, în loc să fie șterse, în conformitate cu legislația națională. Datele	<i>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</i> Anexa nr.1 Punctul 96. În cazul constatării furnizării unor date incorecte, neactuale sau care nu ar fi trebuit furnizate, PUC notifică imediat autoritatea destinatară, asigurând corectarea sau ștergerea acestora fără întârzieri nejustificate. Punctul 99. 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. Punctul 100. Prin derogare de la obligația de ștergere, în cazul în care există motive	Compatibil	

blocate pot fi furnizate sau utilizate doar în scopul care a împiedicat ștergerea lor.	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. Punctul 101. Datele cu caracter personal primite sau furnizate legal de către PUC se șterg din evidențele sale operative: 101.1. imediat ce se constată că nu mai sunt necesare pentru scopul pentru care au fost schimbate; 101.2. la primirea unei notificări de la Punctul Național de Contact (PNC) privind expirarea termenului de păstrare în registrul sursă, conform legislației naționale; 101.3. după expirarea perioadei maxime de păstrare prevăzute în Regulamentul (UE) 2016/794 privind Europol, pentru datele schimbate prin acest canal.		
Articolul 29. Măsuri tehnice și organizatorice de asigurare a protecției și securității datelor (1) Organismele care furnizează date și organismele destinate iau măsurile necesare pentru a asigura protecția eficientă a datelor cu caracter personal împotriva distrugerii accidentale sau neautorizate, pierderii accidentale, accesului neautorizat, modificării neautorizate sau accidentale și divulgării neautorizate.	<i>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</i> Anexa nr.2 Punctul 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. Punctul 38. PNC-urile sunt responsabile de implementarea măsurilor de securitate	Compatibil	

	pentru protejarea integrității și confidențialității datelor în timpul procesului de transmitere către PUC, prin: 38.1. <i>criptarea datelor</i> – PNC-urile utilizează tehnici de criptare corespunzătoare pentru transportul tuturor datelor către Router, EPRIS sau EUCARIS; 38.2. <i>autentificarea securizată</i> – 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; 38.3. <i>protecția fizică și logică</i> – PNC-urile implementează măsuri care să împiedice citirea, copierea, modificarea sau ștergerea neautorizată a suporturilor de date în timpul transportului și prelucrării acestora.		
(2) Elementele specificațiilor tehnice ale procedurii de căutare automatizată sunt reglementate prin măsurile de punere în aplicare menționate la articolul 33, care garantează că: (a) sunt luate măsuri tehnice de ultimă generație în vederea asigurării protecției și securității datelor, în special a confidențialității și integrității acestora; (b) atunci când se recurge la rețele general accesibile sunt utilizate proceduri de criptare și autorizare recunoscute de autoritățile competente; și (c) poate fi verificată admisibilitatea căutărilor, în conformitate cu articolul 30 alineatele (2), (4) și (5).	<i>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</i> Anexa nr. 1 Punctul 101. 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 marcatului în fluxul internațional, conform deciziei PNC sau a CNPDCP. Anexa nr.2	Compatibil	

	Punctul 13. PNC conform ariilor de competență, sunt responsabile de administrarea tehnică, mentenanța și securitatea nodului național conectat la Router-ul Uniunii Europene. Punctul 38. PNC-urile sunt responsabile de implementarea măsurilor de securitate pentru protejarea integrității și confidențialității datelor în timpul procesului de transmitere către PUC, prin: 38.1. <i>criptarea datelor</i> – PNC-urile utilizează tehnici de criptare corespunzătoare pentru transportul tuturor datelor către Router, EPRIS sau EUCARIS; 38.2. <i>autentificarea securizată</i> – 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; 38.3. <i>protecția fizică și logică</i> – PNC-urile implementează măsuri care să împiedice citirea, copierea, modificarea sau ștergerea neautorizată a suporturilor de date în timpul transportului și prelucrării acestora.		
Articolul 30. Introducerea în evidență și înregistrarea; norme speciale care reglementează transmiterea automatizată și neautomatizată (1) Fiecare stat membru garantează că fiecare transmitere neautomatizată și fiecare primire neautomatizată de date cu caracter personal de către organismul care administrează fișierul și de către organismul care efectuează căutarea este introdusă într-o evidență pentru a verifica admisibilitatea		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 45. Norme speciale privind transmiterea automatizată și neautomatizată (1) Punctul național de contact se asigură că orice transmitere și primire neautomatizată de date cu

transmiterii. Luarea în evidență oferă următoarele informații: (a) motivul furnizării datelor; (b) datele furnizate; (c) data furnizării; și (d) numele sau codul de identificare al organismului care efectuează căutarea și al organismului care administrează fișierul.			caracter personal, efectuată de autoritatea care administrează fișierul și care efectuează interogarea, este supusă unei proceduri de înregistrare. Evidența respectivă cuprinde cel puțin următoarele informații: a) temeiul și scopul furnizării datelor; b) datele cu caracter personal transmise; c) data efectuării transmiterii; d) denumirea sau codul de identificare al autorității care efectuează căutarea și care administrează fișierul.
(2) Următoarele dispoziții se aplică în cazul căutărilor automatizate de date în temeiul articolelor 3, 9 și 12 și al comparațiilor automatizate de date în conformitate cu articolul 4: (a) numai agenții punctelor naționale de contact, posesori ai unei autorizații speciale, pot efectua căutări sau comparații automatizate de date. Lista agenților autorizați să efectueze căutări sau comparații automatizate de date se pune la dispoziție la cerere autorităților de supraveghere menționate la alineatul (5), precum și celorlalte state membre. (b) fiecare stat membru se asigură că fiecare transmitere și primire de date cu caracter personal de către organismul care administrează fișierul și de către organismul care efectuează căutarea este înregistrată,		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 45. Norme speciale privind transmiterea automatizată și neautomatizată (2) În cazul interogărilor automatizate de date privind profilurile ADN, datele dactiloscopice și datele de înmatriculare a vehiculelor, precum și al comparațiilor automatizate de profiluri ADN neidentificate, se aplică următoarele reguli: a) interogările și comparațiile automatizate de

comunicând, de asemenea, existența sau lipsa unui „hit” (răspuns pozitiv). Înregistrarea conține următoarele informații: (i) datele furnizate; (ii) data și ora exactă a furnizării; și (iii) numele sau codul de identificare al organismului care efectuează căutarea și al organismului care administrează fișierul. Organismul care efectuează căutarea înregistrează, de asemenea, motivul căutării sau al transmiterii, precum și semnul de identificare al agentului care a efectuat căutarea și al celui care a solicitat căutarea sau transmiterea.		date se efectuează exclusiv de către autoritatea competentă de aplicare a legii, care au drepturi pentru acces și operare. Lista persoanelor autorizate să efectueze căutări sau comparații automatizate se pune la dispoziția autorității naționale de supraveghere competente și, la solicitare, autorităților competente ale statelor participante la schimbul de date; b) punctul național de contact asigură înregistrarea transmiterii și primirii datelor între autoritatea care administrează fișierul și care efectuează căutarea, inclusiv indicarea existenței sau lipsei unui rezultat pozitiv („hit”/„no hit”). Înregistrarea cuprinde cel puțin: datele furnizate, data și ora furnizării și denumirea sau codul de identificare al autorității care efectuează căutarea și care administrează fișierul. (3) Autoritatea competentă de aplicare a legii care efectuează căutarea consemnează motivul căutării ori al transmiterii, precum și identificatorul persoanei autorizate care a efectuat

			căutarea și al persoanei autorizate care a solicitat căutarea ori transmiterea.
(3) La cererea autorităților competente în domeniul protecției datelor din statele membre în cauză, organismul de înregistrare comunică de îndată datele înregistrate, în cel mult patru săptămâni de la data primirii cererii. Datele înregistrate pot fi utilizate doar în următoarele scopuri: (a) monitorizarea protecției datelor; (b) asigurarea securității datelor.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 45. Norme speciale privind transmiterea automatizată și neautomatizată (4) La cererea autorităților competente în domeniul protecției datelor din statele membre în cauză, autoritatea competentă de aplicare a legii comunică datele înregistrate, în cel mult patru săptămâni de la data primirii cererii. Datele înregistrate pot fi utilizate exclusiv în următoarele scopuri: a) monitorizarea respectării cerințelor de protecție a datelor cu caracter personal; b) asigurarea securității datelor.
(4) Datele înregistrate sunt protejate prin adoptarea unor măsuri adecvate împotriva utilizării neautorizate și a altor forme de utilizare incorectă și sunt păstrate timp de doi ani. După expirarea perioadei de păstrare a datelor, datele înregistrate sunt șterse imediat.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 45. Norme speciale privind transmiterea automatizată și neautomatizată

			(5) Datele înregistrate sunt protejate prin aplicarea de măsuri tehnice și organizatorice împotriva utilizării neautorizate și a oricăror forme de utilizare incorectă și se păstrează pe o perioadă de 3 ani, cu excepția înregistrărilor prevăzute la art. 40, care se păstrează pentru termenul special stabilit de acestea. La expirarea termenului de păstrare, datele înregistrate se șterg imediat.
(5) Responsabilitatea controalelor juridice în ceea ce privește transmiterea sau primirea de date cu caracter personal aparține autorităților independente de protecție a datelor sau, dacă este cazul, autorităților judiciare din statele membre în cauză. Oricine poate solicita acestor autorități să verifice legalitatea prelucrării datelor în legătură cu propria persoană, în conformitate cu legislația națională. În afara unor astfel de solicitări, aceste autorități și organismele de înregistrare efectuează controale prin sondaj în ceea ce privește legalitatea furnizărilor, folosind bazele de date respective. Autoritățile independente de protecție a datelor păstrează pentru inspecție rezultatele unor astfel de controale timp de 18 luni. După expirarea acestei perioade, rezultatele în cauză sunt șterse de îndată. Fiecărei autorități de protecție a datelor i se poate solicita de către autoritatea independentă de protecție a datelor dintr-un alt stat membru să își exercite		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 45. Norme speciale privind transmiterea automatizată și neautomatizată (6) Exercitarea controlului de legalitate asupra prelucrării datelor cu caracter personal revine Centrului Național pentru Protecția Datelor cu Caracter Personal sau instanțelor judecătorești competente, după caz. Orice persoană are dreptul să solicite Centrului Național pentru Protecția Datelor cu Caracter Personal verificarea legalității prelucrării datelor care o privesc, în condițiile

atribuțiile în conformitate cu legislația națională. Autoritățile independente de protecție a datelor din statele membre îndeplinesc sarcinile de inspecție necesare cooperării, în special prin intermediul unui schimb de informații relevante.			legislației naționale aplicabile. În lipsa unor asemenea solicitări, Centrul Național pentru Protecția Datelor cu Caracter Personal și entitatea responsabilă de ținerea evidenței efectuează controale privind legalitatea furnizărilor, utilizând bazele de date relevante. (7) Centrul Național pentru Protecția Datelor cu Caracter Personal păstrează pentru verificare rezultatele controalelor efectuate timp de 18 luni, după care le șterge fără întârziere. La solicitarea autorității de protecție a datelor dintr-un al stat, Centrul Național pentru Protecția Datelor cu Caracter Personal își exercită atribuțiile potrivit legislației naționale și îndeplinește sarcinile de inspecție necesare cooperării, inclusiv prin schimbul de informații relevante.
Articolul 31. Drepturile la informații și despăgubiri ale persoanelor vizate (1) La cererea persoanei vizate, în conformitate cu legislația națională, acesteia îi sunt oferite informații, în conformitate cu legislația națională, după dovedirea identității sale, fără cheltuieli excesive, folosind un limbaj inteligibil și fără întârzieri inacceptabile, privind datele prelucrate în ceea		Parțial compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 47. Drepturile la informații și despăgubiri (1) La cererea persoanei, în condițiile cadrului normativ privind protecția datelor cu caracter personal, autoritatea

ce privește persoana sa și originea acestor date, destinatarul sau grupul de destinatari, scopul prelucrării și, în cazul în care acest lucru e necesar în conformitate cu legislația națională, temeiul juridic al prelucrării. De asemenea, persoana vizată are dreptul de a solicita ca datele inexacte să fie corectate și ca datele prelucrate în mod ilegal să fie șterse. Mai mult decât atât, statele membre se asigură că, în cazul încălcării drepturilor sale legate de protecția datelor, persoana vizată poate adresa în mod efectiv o plângere unei instanțe judecătorești independente în sensul articolului 6 alineatul (1) din Convenția europeană a drepturilor omului sau unei autorități independente de supraveghere, în sensul articolului 28 din Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, fiindu-i oferită posibilitatea de a solicita despăgubiri sau de a căuta o altă formă de reparație legală. Normele detaliate privind procedura de exercitare a acestor drepturi și motivele restrângerii dreptului de acces sunt reglementate prin dispozițiile relevante ale legislației naționale a statului membru în care persoana vizată își exercită drepturile.		competentă îi furnizează, fără întârzieri nejustificate, informații privind prelucrarea datelor cu caracter personal care o vizează, după caz: a) categoriile de date prelucrate și originea acestora; b) destinatarul sau categoriile de destinatari; c) scopul prelucrării și, după caz, temeiul juridic al prelucrării. Persoana are dreptul să solicite rectificarea datelor inexacte, completarea datelor incomplete și ștergerea datelor prelucrate ilegal, în condițiile și limitele prevăzute de legislația națională. Persoana are dreptul de a depune o plângere la autoritatea națională de supraveghere competentă și/sau de a se adresa instanței de judecată, în condițiile legii, inclusiv pentru obținerea unei despăgubiri sau a altei forme de reparare a prejudiciului. Condițiile, procedura de exercitare a drepturilor și motivele de restrângere a dreptului de acces se stabilesc potrivit legislației naționale.

			Referirile din textul UE la Directiva 95/46/CE se consideră depășite și neaplicabile, în transpunere se utilizează cadrul național privind protecția datelor aplicabil autorităților competente și dreptul la un remediu efectiv (autoritate de supraveghere/instanță).
(2) În cazul în care un organism dintr-un stat membru a furnizat date cu caracter personal în temeiul prezentei decizii, organismul destinat dintr-un alt stat membru nu poate invoca inexactitatea datelor furnizate drept motiv pentru a se sustrage răspunderii care îi revine față de partea vătămată, în conformitate cu legislația națională. În cazul în care organismul destinat este obligat la plata de despăgubiri ca urmare a faptului că a utilizat date incorecte furnizate, organismul care a furnizat datele restituie organismului destinat întreaga sumă plătită ca despăgubiri.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 47. Drepturile la informații și despăgubiri (2) În cazul în care autoritatea competentă în calitate de autoritate destinatară este obligată, potrivit legii, la plata unor despăgubiri pentru prejudiciul cauzat prin utilizarea unor date cu caracter personal inexacte furnizate de o autoritate competentă dintr-un stat participant, aceasta nu poate invoca inexactitatea datelor furnizate pentru a se exonera de răspundere față de persoana prejudiciată. În situația în care despăgubirea a fost achitată ca urmare a utilizării unor date inexacte furnizate de autoritatea competentă din statul participant, autoritatea

			furnizoare restituie autorității destinate sumă plătită, în condițiile stabilite prin instrumentele de cooperare aplicabile și potrivit procedurilor prevăzute de legislația națională.
Articolul 32. Informații solicitate de statele membre Statul membru destinat să informeze, la cerere, statul membru care furnizează datele cu privire la prelucrarea datelor cu caracter personal furnizate și la rezultatele obținute.	<i>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</i> Anexa nr.1 Punctul 10. PUC acționează ca interfață unică și centralizată între sistemele informaționale naționale și infrastructura centrală a Uniunii Europene, fiind structura administrativă și operațională desemnată la nivel național pentru a asigura fluxul informațional securizat cu statele membre ale Uniunii Europene, alte state și organizațiile internaționale profilate pe schimbul de date și informații de natură infracțională, având următoarele atribuții funcționale și operaționale principale: 10.11. 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.	Compatibil	
Articolul 33. Măsurile de punere în aplicare Consiliul, hotărând cu majoritate calificată după consultarea Parlamentului European, adoptă măsurile necesare punerii în aplicare a prezentei decizii la nivelul Uniunii.		Prevedere UE neaplicabilă	Norma privește adoptarea măsurilor de implementare la nivelul UE (prin Consiliu) pentru aplicarea Deciziei

Articolul 34. Costurile Fiecare stat membru suportă cheltuielile operaționale angajate de autoritățile sale în legătură cu punerea în aplicare a prezentei decizii. În situații speciale, statele membre în cauză pot stabili de comun acord modalități diferite.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 52. Costuri (2) În situații speciale, ce vizează operațiunile comune, misiunile de asistență în caz de dezastre sau detașarea de specialiști, autoritățile competente de aplicare a legii pot stabili de comun acord cu statele membre ale Uniunii Europene vizate modalități de alocare și rambursare a costurilor.
Articolul 35. Relațiile cu alte instrumente (1) Pentru statele membre în cauză, dispozițiile relevante ale prezentei decizii se aplică în locul dispozițiilor corespunzătoare din Tratatul de la Prüm. Oricare alte dispoziții ale Tratatului de la Prüm rămân aplicabile între părțile contractante ale Tratatului de la Prüm.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 55. Aplicarea legii în contextul obligațiilor internaționale (1) Prezenta lege se aplică fără a aduce atingere obligațiilor asumate prin tratatele internaționale la care Republica Moldova este parte. (2) În cazul unui conflict între dispozițiile prezentei legi și cele ale unui tratat internațional, se aplică dispozițiile tratatului internațional, cu excepția situației în care prezenta lege instituie garanții mai favorabile pentru protecția

			drepturilor și libertăților fundamentale.
(2) Fără a aduce atingere angajamentelor asumate în baza altor acte adoptate în conformitate cu titlul VI din tratat: (a) Statele membre pot continua să aplice acordurile sau înțelegerile bilaterale sau multilaterale privind cooperarea transfrontalieră care sunt în vigoare la data adoptării prezentei decizii, în măsura în care astfel de acorduri sau înțelegeri nu sunt incompatibile cu obiectivele prezentei decizii. (b) Statele membre pot încheia sau pune în aplicare acorduri sau înțelegeri bilaterale sau multilaterale privind cooperarea transfrontalieră, după intrarea în vigoare a prezentei decizii, în măsura în care aceste acorduri sau înțelegeri prevăd extinderea sau amplificarea obiectivelor prezentei decizii.		Prevedere UE neaplicabilă	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 55. Aplicarea legii în contextul obligațiilor internaționale (3) Autoritatea competentă de aplicare a legii poate încheia și aplica acorduri/aranjamente bilaterale sau multilaterale de cooperare transfrontalieră, în măsura în care acestea sunt compatibile cu obiectivele prezentei legi și cu obligațiile internaționale asumate. Stabilește efecte și termene interne UE (calendar de aplicare/înlocuire între instrumente) pentru statele membre.
(3) Acordurile și înțelegerile menționate la alineatele (1) și (2) nu pot afecta relațiile cu statele membre care nu sunt părți la acestea.		Prevedere UE neaplicabilă	Dispoziție referitoare la cadrul UE (Titlul VI din Tratat) și la efectele între instrumente ale UE.
(4) În termen de patru săptămâni de la data la care prezenta decizie începe să producă efecte, statele membre informează Consiliul și Comisia în legătură cu acordurile sau înțelegerile existente, în sensul alineatului (2) litera (a), pe care doresc să le aplice în continuare.		Prevedere UE neaplicabilă	Reglementează situații tranzitorii/derogări între statele membre.

(5) De asemenea, statele membre informează Consiliul și Comisia în legătură cu toate noile acorduri sau înțelegeri, în sensul alineatului (2) litera (b), în termen de trei luni de la semnarea acestora sau, în cazul instrumentelor semnate înainte de adoptarea prezentei decizii, în termen de trei luni de la intrarea în vigoare a acestora.		Prevedere UE neaplicabilă	Prevederea continuă regimul tranzitoriu UE (între instrumentele UE și statele membre).
(6) Prezenta decizie nu aduce atingere acordurilor sau înțelegerilor bilaterale sau multilaterale între statele membre și statele terțe.		Prevedere UE neaplicabilă	Vizează modul de operare și efectele juridice în cadrul UE (între state membre) aferente arhitecturii juridice UE.
(7) Prezenta decizie nu aduce atingere acordurilor existente privind asistența judiciară sau recunoașterea reciprocă a hotărârilor judecătorești.		Prevedere UE neaplicabilă	Dispoziție de închidere tranzitorie, specifică contextului UE.
Articolul 36. Punerea în aplicare și declarațiile (1) Statele membre iau măsurile necesare pentru a se conforma dispozițiilor prezentei decizii în termen de un an de la data la care prezenta decizie începe să producă efecte, cu excepția dispozițiilor din capitolul 2 în privința cărora statele membre iau măsurile necesare în termen de trei ani de la data la care prezenta decizie și decizia Consiliului privind punerea în aplicare a acesteia încep să producă efecte.		Prevedere UE neaplicabilă	Prevede termenul UE de conformare pentru statele membre.
(2) Statele membre informează Secretariatul General al Consiliului și Comisia cu privire la punerea în aplicare a obligațiilor care le sunt impuse în baza prezentei decizii și transmit declarațiile prevăzute de prezenta decizie. Odată cu transmiterea acestui text, statul membru poate preciza că va aplica de îndată prezenta decizie în raporturile sale cu		Prevedere UE neaplicabilă	Prevederea instituie obligația statelor membre de a informa Secretariatul General al Consiliului și Comisia și de a transmite „declarații”.

acele state membre care au transmis aceeași notificare.			
(3) Declarațiile depuse în conformitate cu alineatul (2) pot fi modificate în orice moment prin intermediul unei declarații înaintate Secretariatului General al Consiliului. Secretariatul General al Consiliului trimite declarațiile primite statelor membre și Comisiei.		Prevedere UE neaplicabilă	Prevederea reglementează modificarea/retragerea „declarațiilor” în circuitul UE.
(4) Pe baza acestor informații și a altor informații puse la dispoziție de către statele membre, la cerere, Comisia prezintă Consiliului un raport până la 28 iulie 2012 privind punerea în aplicare a prezentei decizii, însoțit de propunerile referitoare la orice alte evoluții ulterioare.		Prevedere UE neaplicabilă	Prevederea reglementează obligația de raportare a Comisiei către Consiliu (mecanism UE de evaluare/monitorizare instituțională).
Articolul 37. Intrarea în vigoare Decizia începe să producă efecte în termen de douăzeci de zile de la data publicării în Jurnalul Oficial al Uniunii Europene.		Prevedere UE neaplicabilă	

TABEL DE CONCORDANȚĂ

la proiectul de Hotărâre 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.	Titlul actului Uniunii Europene, inclusiv cele mai recente amendamente incluse: 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 05.04.2024			
2.	Titlul proiectului de act normativ național: Proiect de Hotărâre 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			
3.	Gradul general de compatibilitate Parțial compatibil			
4.	Autoritatea/persoana responsabilă Ministerul Afacerilor Interne			
5.	Data întocmirii/actualizării 15.05.2026			
6. Actul Uniunii Europene		7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observații
Articolul 1. Obiectul Prezentul regulament stabilește un cadru pentru căutarea și schimbul de informații între autoritățile competente din statele membre (denumit în continuare „cadru Prüm II”) prin stabilirea: (a) condițiilor și procedurilor pentru căutarea automatizată de profiluri ADN, de date dactiloscopice, de anumite date privind înmatricularea vehiculelor, de imagini faciale și de evidențe ale poliției; și (b) normelor privind schimbul de date de bază în urma unei concordanțe confirmate de date biometrice.			Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 1. Obiectul de reglementare (2) Prezenta lege stabilește norme privind: a) desemnarea punctului unic de contact, organizarea, atribuțiile, și componența acestuia; b) schimbul de date cu privire la căutarea directă sau automatizată de profiluri ADN, date dactiloscopice, date privind vehicule precum și piesele componente ale acestuia

			consemnate cu număr de identificare, imagini faciale, date privind documente de călătorie declarate furate, pierdute, revocate, nevalidate sau blancurile documentelor furate înainte de emitere, evidențe ale poliției, datele personale ale persoanelor străine sau cetățenilor Republicii Moldova urmăriți internațional, aflați în vizorul autorităților de aplicare a legii, datele biometrice și antropometrice necesare identificării persoanelor dispărute fără veste, cadavrelor și părților acestuia, precum și alte date care fac obiectul schimbului de date de interes polițienesc; c) normele privind schimbul de informații în urma confirmării unei concordanțe în datele biometrice (mecanismul hit/no-hit);
Articolul 2. Scopul Scopul cadrului Prüm II este de a intensifica cooperarea transfrontalieră în domeniile reglementate de partea III titlul V capitolele 4 și 5 din Tratatul privind funcționarea Uniunii Europene, în special prin facilitarea schimbului de informații între autoritățile competente ale statelor membre, cu respectarea deplină a drepturilor fundamentale ale persoanelor fizice, inclusiv dreptul la viață privată și dreptul la protecția datelor cu caracter personal, în conformitate		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 2. Scopul legii și domeniul de aplicare (4) Categoriile de date care fac obiectul schimbului informațional internațional, inclusiv automatizat sunt: a) date de identificare nominală și biometrice ale persoanelor, inclusiv profiluri ADN, date dactiloscopice și imagini faciale,

cu Carta drepturilor fundamentale a Uniunii Europene. De asemenea, cadrul Prüm II are scopul de a le permite autorităților competente din statele membre să efectueze căutări ale persoanelor dispărute în contextul anchetelor penale sau din motive umanitare și să identifice rămășițe umane, în conformitate cu articolul 29, cu condiția ca autoritățile respective să fie împuternicite să efectueze astfel de căutări și să efectueze o astfel de identificare în temeiul dreptului intern.			în scopul localizării persoanelor dispărute fără veste, identificării cadavrelor sau părților acestuia sau urmăririi persoanelor în vederea arestării și extrădării; b) date privind mijloacele de transport, inclusiv autovehiculele anunțate în căutare, precum și piesele componente ale acestora identificate prin număr de serie; c) date privind armele de foc, munițiile și materialele explozive, inclusiv cele declarate pierdute, furate sau utilizate în comiterea de infracțiuni; d) date privind documentele de călătorie, vizele, titlurile de valoare, inclusiv a celor declarate false, furate sau pierdute.
Articolul 3. Domeniul de aplicare Prezentul regulament se aplică bazelor de date instituite în conformitate cu dreptul intern și utilizate pentru transferul automatizat al profilurilor ADN, al datelor dactiloscopice, al anumitor date privind înmatricularea vehiculelor, al imaginilor faciale și al evidențelor poliției, în conformitate cu Directiva (UE) 2016/680 sau cu Regulamentul (UE) 2018/1725, (UE) 2016/794 sau (UE) 2016/679, după caz.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 6. Punctul unic de contact și atribuțiile acestuia (1) Se desemnează în calitate de punct unic de contact pentru cooperarea polițienească internațională subdiviziunea specializată în cooperare polițienească internațională din subordinea Inspectoratului General al Poliției al Ministerului Afacerilor Interne. (2) Punctul unic de contact asigură cooperarea cu punctele naționale de contact desemnate

			prin hotărâre de Guvern, din cadrul autorităților competente naționale, pe următoarele domenii: a) profiluri ADN; b) date dactiloscopice; c) date referitoare la mijloace de transport, inclusiv autovehicule anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale; d) imagini faciale; e) evidențe polițienești, inclusiv date nominale privind persoanele urmărite, dispărute sau implicate în activități infracționale;
Articolul 4. Definiții În sensul prezentului regulament, se aplică următoarele definiții:		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 3. Noțiuni principale (1) Noțiunile din prezenta lege se definesc în conformitate cu Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară, Legea nr. 1549/2002 cu privire la înregistrarea dactiloscopică de stat, Legea nr. 195/2024 privind protecția datelor cu caracter personal, Legea nr. 48/2023 privind securitatea cibernetică, Legea nr. 273/1994 privind actele de identitate din sistemul național de pașapoarte, Legea nr. 248/2025 privind managementul situațiilor

		de criză și Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate. (2) În sensul prezentei legi, termenii și expresiile de mai jos au următoarele semnificații: 1) <i>autoritate competentă</i> – autoritate publică, instituție sau altă entitate abilitată prin lege să exercite atribuții în domeniile reglementate de prezenta lege. 2) <i>autoritate competentă de aplicare a legii</i> – autoritate polițienească, judiciară, vamală sau altă autoritate de aplicare a legii, din Republica Moldova sau din alte țări, cu atribuții în prevenirea, depistarea sau investigarea infracțiunilor. 3) <i>autoritate de supraveghere</i> – autoritate publică independentă care asigură supravegherea și monitorizarea aplicării legislației privind protecția datelor cu caracter personal și a altor acte normative în domeniu, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor în legătură cu prelucrarea datelor cu caracter personal; 4) <i>baze de date INTERPOL</i> – ansamblul sistemelor informaționale și al registrelor centralizate, gestionate de Secretariatul General al Organizației Internaționale a

		Poliției Criminale (INTERPOL), care conțin date cu caracter personal, date biometrice (profiluri ADN, date dactiloscopice, imagini faciale, ș.a) și informații operative privind obiecte, documente sau activități infracționale, puse la dispoziția statelor membre în scopul schimbului de informații pentru prevenirea și combaterea criminalității transfrontaliere; 6) <i>Biroul Național SIRENE</i> - unitate operațională care funcționează în regim de 24/7 în calitate de punct de contact pentru statele membre ale Uniunii Europene, în scopul asigurării schimbului de informații suplimentare privind introducerea semnalărilor în Sistemul de informații Schengen, pentru a permite luarea măsurilor adecvate în cazul în care persoanele sau obiectele care fac obiectul unei semnalări în Sistemul de informații Schengen sunt localizate în urma generării unei concordanțe sau obținerii unui rezultat pozitiv; 7) <i>blocare de date</i> – marcarea prin acoperire a datelor cu caracter personal stocate, cu scopul de a limita prelucrarea lor ulterioară; 8) <i>cerere de informații</i> - solicitarea de date și informații

		formulată în scopul prevenirii, depistării sau investigării infracțiunilor, astfel cum acesta rezultă din tratatele internaționale și din actele normative relevante ale Uniunii Europene; 9) <i>concordanță (hit)</i> – rezultatul pozitiv generat de un sistem informatic în momentul în care datele introduse pentru căutare/interogare de către o autoritate de aplicare a legii coincid cu datele deja existente într-o bază de date internațională sau națională referitoare la o persoană, un vehicul sau un obiect; 10) <i>date alfanumerice</i> – date constând în litere, cifre, caractere speciale, spații și semne de punctuație; 11) <i>date Europol</i> – orice date operaționale cu caracter personal prelucrate de Europol, statele membre și statele partenere, în conformitate cu mandatul Europol; 12) <i>date Interpol</i> – totalitatea datelor prelucrate de către statele membre ale INTERPOL și alte entități, prin canalele și bazele de date ale Organizației Internaționale a Poliției Criminale - INTERPOL, în conformitate cu regulile acestora privind prelucrarea datelor;

		13) <i>date de referință privind imaginea facială</i> – imagine facială și numărul de referință menționat la art. 17, alin. (1), utilizate pentru compararea și schimbul automatizat al datelor, fără a permite identificarea directă a persoanei; 14) <i>EPRIS</i> - Sistemul european de inventariere a evidențelor poliției, utilizat de statele membre ale Uniunii Europene și Europol pentru căutarea automatizată în registrele naționale ale evidențelor poliției; 15) <i>EUCARIS</i> - Sistemul de informații european privind vehiculele și permisele de conducere; 16) <i>eveniment major cu dimensiune transfrontalieră</i> - eveniment cu caracter internațional, precum competiții sportive internaționale, reuniuni la nivel înalt, summituri, conferințe internaționale, manifestări culturale ori religioase de amploare sau alte adunări publice similare, dar fără a se limita la acestea, care, prin participarea numeroasă, importanța publică ori expunerea mediatică, pot genera riscuri la adresa ordinii și siguranței publice și impun cooperarea autorităților

		competente de aplicare a legii din două sau mai multe state; 17) <i>evidențe ale poliției</i> – date biografice ale bănușilor, învinușilor, inculpașilor și condamnașilor, disponibile în bazele de date nașionale instituite în scopul prevenirii, depistării și investigării infracșunilor; 18) <i>informașii</i> - orice conșinut, documente, evidenșe, activitași sau rapoarte, indiferent de suport, formă, mod de exprimare sau de punere în circulașie, referitoare la una sau mai multe persoane fizice sau juridice, fapte sau circumstanșe relevante pentru autoritașile competente în scopul îndeplinirii atribușilor care le revin în domeniul prevenirii, depistării sau investigării infracșunilor, inclusiv informașii operașionale în materie penală; 19) <i>imagine facială</i> – imagine digitală a feșei unei persoane; 20) <i>imagine facială identificată</i> – imaginea facială a unei persoane identificate; 21) <i>imagine facială neidentificată</i> – imagine facială colectată în cadrul prevenirii, constatașii sau investigării unei infracșuni ori în cadrul căutării unei persoane dispărute fără veste sau al identificării cadavrelor sau părșilor acestuia, care nu este

		asociată, la momentul introducerii, unei persoane identificate; 22) <i>procedura de căutare automatizată</i> – modalitatea tehnică de acces direct și simultan la bazele de date naționale sau internaționale, care permite autorităților competente să verifice existența unei concordanțe (hit) printr-o interogare informatică, oferind un răspuns imediat de tip „pozitiv/negativ” (<i>hit/no-hit</i>). 23) <i>punct național de contact</i> - autoritate competentă desemnată în temeiul art. 6 alin. (2) din prezenta lege, responsabilă de gestionarea tehnică și administrarea schimbului automatizat pentru o categorie specifică de date; 24) <i>punct unic de contact</i> - structură centrală desemnată în temeiul art. 6 alin. (1) din prezenta lege, responsabilă de coordonarea strategică și operațională la nivel național, monitorizarea fluxurilor de informații și asigurarea cooperării polițienești internaționale în regim de 24/7; 25) <i>router</i> - infrastructura tehnică centralizată instituită și gestionată de Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Domeniul Libertății, Securității și

			Justiției (eu-LISA), care asigură transmiterea și rutarea automatizată a căutărilor și a schimbului de date biometrice, profiluri ADN și date dactiloscopice, precum și imaginile faciale între statele membre și Europol; 26) <i>SIENA</i> (acronim pentru <i>Secure Information Exchange Network Application</i>) – canalul de comunicații securizat, gestionat de Europol, destinat schimbului de informații operative și strategice între statele membre ale Uniunii Europene, Europol și statele partenere; 27) <i>Sistemul de Informații Schengen (SIS)</i> – sistemul informatic centralizat, de scară largă, destinat cooperării polițienesci și al cooperării judiciare în materie penală, controlului la trecerea frontierelor și returnărilor; 28) <i>SLTD</i> (acronim pentru <i>Stolen and Lost Travel Documents</i>) – baza de date internațională gestionată de Secretariatul General al INTERPOL, care conține informații despre documentele de călătorie (pașapoarte, cărți de identitate, vize) și formularele de documente oficiale care au fost

			raportate ca fiind furate, pierdute, nevalidate sau furate; 29) <i>stat solicitant</i> – statul care formulează o cerere de informații în sensul prezentei legi; 30) <i>stat solicitat</i> – statul căruia îi este adresată o cerere de informații în sensul prezentei legi; 31) <i>stat participant</i> – stat membru al Uniunii Europene, stat asociat spațiului Schengen ori, după caz, alt stat cu care Republica Moldova realizează forme de cooperare polițienească și schimb de date în temeiul tratatelor internaționale aplicabile și al actelor normative speciale. 32) <i>suspect</i> – persoana în privința căreia există motive serioase să se creadă că a săvârșit sau că urmează să săvârșască o infracțiune; 33) <i>sistem de schimb automatizat de date</i> – mecanism tehnic de interconectare a sistemelor informaționale, care permite efectuarea de căutări automatizate și schimbul de date între autorități competente de aplicare a legii, pe baza unei concordanțe, fără a acorda acces direct la conținutul bazelor de date.
„loci” (singular: „locus”) înseamnă segmente de ADN care conțin caracteristicile		Compatibil	Art. 2 din Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară

de identificare a unei mostre de ADN uman analizate.			„loci” (singular: „locus”) – segmente de ADN care conțin caracteristicile de identificare a unei mostre de ADN uman analizate.
„profil ADN” înseamnă un cod alfabetic sau numeric care reprezintă un set de loci sau structura moleculară specifică din diverși loci.		Compatibil	Art. 2 din Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară profil ADN – cod format din litere sau din cifre, care reprezintă un set de caracteristici de identificare a părții necodificate a unui eșantion analizat de ADN uman, precum și structura moleculară specifică din diverse segmente de ADN (loci).
„date de referință ADN” înseamnă un profil ADN și numărul de referință menționat la articolul 7.		Compatibil	Art. 2 din Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară date de referință ADN – profilul ADN și numărul de referință.
„profil ADN identificat” înseamnă profilul ADN al unei persoane identificate.		Compatibil	Proiectul de lege privind cooperarea polițienească internațională prevede și completarea Legii nr. 235/2017 cu privire la înregistrarea genetică judiciară, cu noțiunea „profil ADN identificat” . Articolul 2. Noțiuni principale „profil ADN identificat” – profilul ADN al unei persoane identificate;
„profil ADN neidentificat” înseamnă profilul ADN colectat în cursul investigării unor infracțiuni și care aparține unei persoane		Compatibil	Art. 2 din Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară

încă neidentificate, inclusiv profilul ADN obținut din urme.			<i>profil ADN neidentificat</i> – profil ADN obținut din indiciile culese în timpul investigării unor infracțiuni și care aparține unei persoane neidentificate;
„date dactiloscopice” înseamnă imagini de amprente digitale, imagini de amprente digitale latente, imagini de amprente palmare, imagini de amprente palmare latente și șabloane ale unor astfel de imagini (caracteristici codificate ale acestora) care sunt stocate și prelucrate într-o bază de date automatizată.		Compatibil	Art. 2 din Legea nr. 1549/2002 cu privire la înregistrarea dactiloscopică de stat <i>date dactiloscopice</i> – imagini de amprente digitale, imagini de amprente digitale latente, imagini de amprente palmare, imagini de amprente palmare latente, precum și caracteristici codificate ale unor astfel de imagini stocate și procesate într-o bază de date electronică;
„date dactiloscopice de referință” înseamnă date dactiloscopice și numărul de referință menționat la articolul 12.		Compatibil	Proiectul de lege privind cooperarea polițienească internațională prevede și completarea Legii nr. 1549/2002 cu privire la înregistrarea dactiloscopică de stat, cu noțiunea „date dactiloscopice de referință”. Articolul 2. Noțiuni principale <i>date dactiloscopice de referință</i> - număr format din combinația următoarelor elemente: a) un cod care să permită identificarea și extragerea datelor cu caracter personal și a altor informații din Sistemul informațional automatizat „Registrul de stat dactiloscopic”;

			b) un cod care să indice originea națională a datelor dactiloscopice.
„date dactiloscopice neidentificate” înseamnă datele dactiloscopice colectate în cursul investigării unei infracțiuni și care aparțin unei persoane neidentificate încă, inclusiv datele dactiloscopice obținute din urme.		Compatibil	Proiectul de lege privind cooperarea polițienească internațională prevede și completarea Legii nr. 1549/2002 cu privire la înregistrarea dactiloscopică de stat, cu noțiunea de „date dactiloscopice neidentificate”. Articolul 2. Noțiuni principale <i>date dactiloscopice neidentificate</i> - datele dactiloscopice colectate în cursul investigării unei infracțiuni și care aparțin unei persoane neidentificate încă, inclusiv datele dactiloscopice obținute din urme.
„date dactiloscopice identificate” înseamnă datele dactiloscopice ale unei persoane identificate		Compatibil	Proiectul de lege privind cooperarea polițienească internațională prevede și completarea Legii nr. 1549/2002 cu privire la înregistrarea dactiloscopică de stat, cu noțiunea de „date dactiloscopice identificate”. Articolul 2. Noțiuni principale <i>date dactiloscopice identificate</i> - datele dactiloscopice ale unei persoane identificate.
„caz individual” înseamnă un dosar unic legat de prevenirea, depistarea sau investigarea unei infracțiuni, de căutarea unei persoane dispărute sau de identificarea unor rămășițe umane neidentificate.		Compatibil	Proiectul de lege privind cooperarea polițienească internațională prevede și completarea Legii nr. 235/2017 cu privire la înregistrarea genetică

			judiciară, cu noțiunea „caz individual”. Articolul 2. Noțiuni principale caz individual – dosar unic legat de prevenirea, depistarea sau investigarea unei infracțiuni, de căutarea unei persoane dispărute sau de identificarea unor rămășițe umane neidentificate.
„date biometrice” înseamnă profiluri ADN, date dactiloscopice sau imagini faciale.		Compatibil	Art. 4 din Legea nr. 195/2024 privind protecția datelor cu caracter personal. <i>date biometrice</i> – date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice.
„pseudonimizare” înseamnă pseudonimizarea în înțelesul definiției de la articolul 3 punctul 5 din Directiva (UE) 2016/680		Compatibil	Art. 4 din Legea nr. 195/2024 privind protecția datelor cu caracter personal <i>pseudonimizare</i> – prelucrare a datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică

			care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile.
„date cu caracter personal” înseamnă datele cu caracter personal în înțelesul definiției de la articolul 3 punctul 1 din Directiva (UE) 2016/680		Compatibil	<i>Art. 4 din Legea nr. 195/2024 privind protecția datelor cu caracter personal</i> <i>date cu caracter personal</i> – orice informații privind o persoană fizică identificată sau identificabilă (în continuare – persoană vizată). Persoana fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special, prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul ori mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.
„incident” înseamnă un incident în înțelesul definiției de la articolul 6 punctul 5 din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului		Compatibil	<i>Art. 2 Legea nr. 48/2023 privind securitatea cibernetică</i> <i>incident cibernetic</i> – eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețelele și sistemele informatice sau accesibile prin intermediul acestora;
„incident semnificativ” înseamnă orice incident, cu excepția cazului în care		Compatibil	<i>Proiectul de lege privind cooperarea polițienească</i>

respectivul incident are un impact redus și este probabil să fie deja bine înțeles în ceea ce privește metoda sau tehnologia;			<i> internațională </i> prevede și completarea Legii nr. 48/2023 privind securitatea cibernetică, cu noțiunea „incident semnificativ” Articolul 2. Noțiuni principale „incident semnificativ” orice incident, cu excepția celor care au un impact redus și a căror natură, metodă sau tehnologie utilizată sunt deja cunoscute și bine înțelese, astfel încât nu generează riscuri noi sau relevante.
„amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică care are oportunitatea și vocația de a provoca un incident semnificativ, și care are un asemenea scop;		Compatibil	Art. 2 Legea nr. 48/2023 privind securitatea cibernetică <i> amenințare cibernetică semnificativă </i> – amenințare cibernetică despre care se poate presupune, pe baza caracteristicilor tehnice ale acesteia, că are potențialul de a afecta grav rețelele și sistemele informatice ale unei persoane juridice care prestează servicii sau utilizatorii serviciilor furnizate de aceasta, cauzând prejudicii materiale și/sau nonmateriale considerabile.
Articolul 5. Date ADN de referință (1) Statele membre asigură disponibilitatea datelor de referință ADN din bazele lor de date ADN naționale în scopul efectuării de căutări automatizate de către alte state membre și de către Europol în temeiul prezentului regulament.		Compatibil	Proiectul de lege pentru cooperarea polițienească internațională Articolul 10. Date ADN de referință (1) Autoritatea competentă de aplicare a legii asigură punerea la dispoziție a profilurilor ADN

Datele de referință ADN nu conțin niciun fel de date suplimentare care să permită identificarea directă a unei persoane. Profilurile ADN neidentificate trebuie să poată fi recunoscute ca atare.			stocate în Registrul de stat al datelor genetice, pentru efectuarea căutării automatizate în bazele de date de către autoritățile statelor membre ale Uniunii Europene și de Europol, în condițiile prezentei legi. (2) Datele de referință ADN puse la dispoziție nu conțin date care să permită identificarea directă a persoanei, iar profilurile ADN neidentificate se marchează distinct și sunt recunoscute ca atare în sistem.
(2) Datele ADN de referință se prelucrează în conformitate cu prezentul regulament și cu respectarea dreptului intern aplicabil procedurii de prelucrare a datelor respective.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 10. Date ADN de referință (3) Prelucrarea datelor de referință ADN se realizează în conformitate cu prevederile prezentei legi și cu respectarea procedurii de prelucrare a datelor respective în conformitate cu legislația privind protecția datelor cu caracter personal.
(3) Comisia adoptă un act de punere în aplicare pentru a preciza caracteristicile de identificare ale unui profil ADN care face obiectul schimbului de date. Respectivul act de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).		Prevedere UE neaplicabilă	Prevedere privind adoptarea de către Comisia Europeană a unui act de punere în aplicare și procedura de examinare (art. 77 alin. (2)) are caracter instituțional specific UE.

Articolul 6. Căutarea automatizată a profilurilor ADN (1) În scopul investigării infracțiunilor, statele membre efectuează, la momentul primei conectări la router prin intermediul punctelor lor de contact naționale, o căutare automatizată, comparând toate profilurile ADN stocate în bazele lor de date ADN cu toate profilurile ADN stocate în bazele de date ADN ale tuturor celorlalte state membre și cu datele Europol. Fiecare stat membru convine la nivel bilateral cu fiecare alt stat membru și cu Europol cu privire la modalitățile de efectuare a respectivelor căutări automatizate, în conformitate cu normele și procedurile prevăzute în prezentul regulament.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 11. Căutarea automatizată a profilurilor ADN (1) În scopul prevenirii, depistării și investigării infracțiunilor, la momentul primei conectări la infrastructura tehnică prevăzută de prezenta lege, punctul național de contact efectuează o comparare integrală a profilurilor ADN din Registrul de stat al datelor genetice cu profilurile ADN stocate în bazele de date ale statelor membre ale Uniunii Europene și ale Europol.
(2) În scopul investigării infracțiunilor, statele membre, prin intermediul punctelor lor de contact naționale, efectuează căutări automatizate, comparând toate profilurile ADN nou adăugate în baza lor de date ADN cu toate profilurile ADN stocate în bazele de date ADN ale tuturor celorlalte state membre și cu datele Europol.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 11. Căutarea automatizată a profilurilor ADN (2) După realizarea conectării, punctul național de contact asigură căutarea automatizată prin compararea profilurilor ADN nou introduse în Registrul de stat al datelor genetice cu profilurile ADN stocate în bazele de date ADN ale altor state membre ale UE și cu datele Europol.
(3) În cazul în care căutările, astfel sunt menționate la alineatul (2), nu pot avea loc, statul membru în cauză poate conveni la nivel bilateral cu fiecare alt stat membru și cu Europol să le efectueze într-o etapă ulterioară,		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 11. Căutarea automatizată a profilurilor ADN

comparând profilurile ADN cu toate profilurile ADN stocate în bazele de date ADN ale tuturor celorlalte state membre și cu datele Europol. Statul membru în cauză convine la nivel bilateral cu fiecare alt stat membru și cu Europol cu privire la modalitățile de efectuare a respectivelor căutări automatizate, în conformitate cu normele și procedurile prevăzute în prezentul regulament.			(3) Dacă căutările automatizate menționate la alin. (2) nu pot fi efectuate, punctul național de contact poate conveni, la nivel bilateral, cu statul membru vizat sau cu Europol, efectuarea acestora într-o etapă ulterioară, prin compararea profilurilor ADN nou adăugate cu profilurile stocate în bazele de date ale statelor membre implicate sau ale Europol.
(4) Căutările, astfel cum sunt menționate la alineatele (1), (2) și (3) se efectuează numai în cadrul unor cazuri individuale și în conformitate cu dreptul intern al statului membru solicitant.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 11. Căutarea automatizată a profilurilor ADN (4) Căutările menționate la alin. (1)-(3) se efectuează exclusiv în cazuri individuale, cu respectarea prezentei legi și a normelor privind protecția datelor cu caracter personal.
(5) În cazul în care o căutare automatizată indică o concordanță între un profil ADN furnizat și un profil ADN stocat în baza de date sau în bazele de date ale statului membru solicitat în care se efectuează căutarea, punctul de contact național al statului membru solicitant primește o notificare automatizată a datelor de referință ADN în raport cu care a fost identificată o concordanță.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 11. Căutarea automatizată a profilurilor ADN (5) În cazul identificării unei concordanțe („hit”) între un profil ADN transmis și un profil ADN stocat într-o bază de date a unui stat membru sau a statului membru solicitat, punctul național de contact primește o notificare automatizată care conține datele de referință ale profilului ADN

			corespunzător pentru care a fost identificată concordanța.
(6) Punctul de contact național al statului membru solicitant poate decide să confirme o concordanță între două profiluri ADN. Dacă decide să confirme o concordanță între două profiluri ADN, acesta informează statul membru solicitat și se asigură că se efectuează o revizuire manuală de către cel puțin un membru calificat al personalului pentru a confirma respectiva concordanță cu datele de referință ADN primite de la statul membru solicitat.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 11. Căutarea automatizată a profilurilor ADN (7) Confirmarea concordanței între două profiluri ADN se realizează prin revizuire manuală de către un expert sau specialist în genetică judiciară din cadrul subdiviziunii responsabile de administrarea Registrului de stat al datelor genetice, calificat potrivit legislației naționale și procedurilor interne aplicabile. (8) În cazul în care confirmarea este realizată de autoritatea competentă de aplicare a legii a Republicii Moldova, punctul național de contact informează statul membru sau Europol cu privire la rezultatul revizuirii manuale.
(7) Dacă este relevant în scopul investigării infracțiunilor, punctul de contact național al statului membru solicitat poate decide să confirme o concordanță între două profiluri ADN. Dacă decide să confirme o concordanță între două profiluri ADN, acesta informează statul membru solicitant și se asigură că se efectuează o revizuire manuală de către cel puțin un membru calificat al personalului pentru a confirma respectiva		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 11. Căutarea automatizată a profilurilor ADN (6) Notificarea automată a concordanței se generează numai dacă este întrunit pragul minim de loci stabilit potrivit cerințelor tehnice aplicabile.

concordanță cu datele de referință ADN primite de la statul membru solicitant.			
Articolul 7. Numerele de referință pentru profilurile ADN Numerele de referință pentru profilurile ADN reprezintă combinația dintre: a) un număr de referință care permite statelor membre, în cazul unei concordanțe, să extragă date suplimentare și alte informații din bazele lor de date naționale ADN pentru a le furniza unuia, mai multor sau tuturor celorlalte state membre, în conformitate cu articolul 47, sau către Europol, în conformitate cu articolul 49 alineatul (6); b) un număr de referință care permite Europol ca, în cazul unei concordanțe, să extragă date suplimentare și alte informații în sensul articolului 48 alineatul (1) din prezentul regulament pentru a le furniza unuia, mai multor sau tuturor statelor membre, în conformitate cu Regulamentul (UE) 2016/794; c) un cod care indică statul membru care deține profilul ADN; (d) un cod care indică dacă profilul ADN este un profil ADN identificat sau un profil ADN neidentificat.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> prevede și completarea <i>Legii nr. 235/2017 cu privire la înregistrarea genetică judiciară, noțiunea „numere de referință” se substituie cu noțiunea „date de referință”.</i> Articolul 2. Noțiuni principale <i>date de referință ADN</i> – număr format din combinația următoarelor elemente: a) număr de referință care permite identificarea profilului ADN corespunzător în Registrul de stat al datelor genetice în cazul unei concordanțe, în vederea furnizării ulterioare de date suplimentare potrivit procedurilor legale aplicabile; b) număr de referință care, care permite asocierea profilului ADN cu fluxurile de schimb de date realizate prin intermediul Europol, în condițiile dreptului Uniunii Europene și ale cadrului normativ național; c) un cod care indică originea națională a profilului ADN; d) un cod care indică caracterul identificat sau neidentificat al profilului ADN. Numărul de referință nu permite identificarea directă a unei

			persoane și nu oferă acces automat la date cu caracter personal. Totodată, prevederile urmează să se regăsească inclusiv în <i>proiectul de modificare a Hotărârii de Guvern nr. 821/2023 pentru aprobarea Conceptului Sistemului informațional „Registrul de stat al datelor genetice” și a Regulamentului privind modalitatea de ținere a Registrului de stat al datelor genetice.</i>
Articolul 8. Principii privind schimbul de profiluri ADN (1) Statele membre iau măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea datelor de referință ADN trimise către alte state membre sau Europol, inclusiv criptarea acestora. Europol ia măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea datelor de referință ADN trimise către state membre, inclusiv criptarea acestora.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 821/2023 pentru aprobarea Conceptului Sistemului informațional „Registrul de stat al datelor genetice” și a Regulamentului privind modalitatea de ținere a Registrului de stat al datelor genetice</i>
(2) Fiecare stat membru și Europol se asigură că profilurile ADN pe care le transmite sunt de o calitate suficientă pentru a permite compararea automatizată. Comisia stabilește, prin intermediul actelor de punere în aplicare, un standard minim de calitate care să permită compararea profilurilor ADN.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 821/2023 pentru aprobarea Conceptului Sistemului informațional „Registrul de stat al datelor genetice” și a Regulamentului privind modalitatea de ținere a Registrului de stat al datelor genetice.</i>

			Partea a doua a normei privind stabilirea de către Comisia Europeană, prin acte de punere în aplicare, a unui standard minim de calitate are caracter instituțional UE.
(3) Comisia adoptă acte de punere în aplicare prin care precizează standardele europene sau internaționale relevante care trebuie utilizate de către statele membre și Europol pentru schimbul de date de referință ADN.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 821/2023 pentru aprobarea Conceptului Sistemului informațional „Registrul de stat al datelor genetice” și a Regulamentului privind modalitatea de ținere a Registrului de stat al datelor genetice.</i> Partea a doua a normei privind adoptarea de către Comisia Europeană a actelor de punere în aplicare pentru precizarea standardelor europene/internaționale relevante este specifică UE
(4) Actele de punere în aplicare menționate la alineatele (2) și (3) de la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).		Prevedere UE neaplicabilă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 821/2023 pentru aprobarea Conceptului Sistemului informațional „Registrul de stat al datelor genetice” și a Regulamentului privind modalitatea de ținere a</i>

			<i>Registrului de stat al datelor genetice.</i> Dispoziția se referă la adoptarea de către Comisia Europeană a actelor de punere în aplicare conform procedurii de comitologie. Reglementează un proces instituțional al Uniunii Europene și nu stabilește obligații sau competențe pentru autoritățile naționale.
Articolul 9. Norme privind solicitările și răspunsurile referitoare la profilurile ADN (1) O solicitare de căutare automatizată a profilurilor ADN include numai informațiile următoare: (a) codul statului membru solicitant; (b) data și ora solicitării și numărul solicitării; (c) datele de referință ADN; (d) dacă profilurile ADN transmise sunt profiluri ADN neidentificate sau profiluri ADN identificate.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 821/2023 pentru aprobarea Conceptului Sistemului informațional „Registrul de stat al datelor genetice” și a Regulamentului privind modalitatea de ținere a Registrului de stat al datelor genetice.</i>
(2) Un răspuns la o solicitare astfel cum este menționată la alineatul (1) conține numai informațiile următoare: (a) o precizare din care să reiasă dacă a existat una sau au existat mai multe concordanțe sau dacă nu a existat nicio concordanță; (b) data și ora solicitării și numărul solicitării; (c) data și ora răspunsului și numărul răspunsului;		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 821/2023 pentru aprobarea Conceptului Sistemului informațional „Registrul de stat al datelor genetice” și a Regulamentului privind modalitatea de ținere a Registrului de stat al datelor genetice.</i>

(d) codul statului membru solicitant și cel al statului membru solicitat; (e) numerele de referință ale profilurilor ADN din statul membru solicitant și din statul membru solicitat; (f) dacă profilurile ADN transmise sunt profiluri ADN neidentificate sau profiluri ADN identificate; (g) profilurile ADN între care s-a stabilit o concordanță.			
(3) O concordanță se notifică automat numai dacă în urma căutării automatizate a rezultat o concordanță cu un număr minim de loci. Comisia adoptă acte de punere în aplicare prin care precizează numărul minim de loci în acest scop, în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).		Parțial compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 11. Căutarea automatizată a profilurilor ADN (6) Notificarea automată a concordanței se generează numai dacă este întrunit pragul minim de loci stabilit potrivit cerințelor tehnice aplicabile. Determinarea numărului minim de loci și regulile tehnice aferente se va transpune prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 821/2023 pentru aprobarea Conceptului Sistemului informațional „Registrul de stat al datelor genetice” și a Regulamentului privind modalitatea de ținere a Registrului de stat al datelor genetice.</i>
(4) În cazul în care o căutare de profiluri ADN neidentificate conduce la o concordanță,		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui

fiecare stat membru solicitat care deține date cu care s-a stabilit concordanța poate introduce în baza sa de date națională un marcaj care să indice că a existat o concordanță pentru profilul ADN respectiv în urma căutării efectuate de un alt stat membru. Marcajul include numărul de referință al profilului ADN utilizat de statul membru solicitant.			<i>proiect de modificare a Hotărârii de Guvern nr. 821/2023 pentru aprobarea Conceptului Sistemului informațional „Registrul de stat al datelor genetice” și a Regulamentului privind modalitatea de ținere a Registrului de stat al datelor genetice.</i>
(5) Statele membre se asigură că solicitările menționate la alineatul (1) de la prezentul articol sunt corelate cu notificările transmise în temeiul articolului 74. Notificările respective se reproduc în manualul practic menționat la articolul 79.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 821/2023 pentru aprobarea Conceptului Sistemului informațional „Registrul de stat al datelor genetice” și a Regulamentului privind modalitatea de ținere a Registrului de stat al datelor genetice.</i>
Articolul 10. Date dactiloscopice de referință (1) Statele membre asigură disponibilitatea datelor dactiloscopice de referință din bazele lor de date naționale instituite în scopul prevenirii, depistării și investigării infracțiunilor.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 13. Date dactiloscopice de referință (1) În scopul prevenirii, depistării și investigării infracțiunilor, autoritatea competentă de aplicare a legii, asigură disponibilitatea, pentru efectuarea căutărilor automatizate a datelor dactiloscopice de referință stocate în Registrul de stat dactiloscopic.

(2) Datele dactiloscopice de referință nu conțin niciun fel de date suplimentare care să permită identificarea directă a unei persoane.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 13. Date dactiloscopice de referință (2) Datele dactiloscopice de referință utilizate pentru schimbul automatizat de date conțin datele necesare efectuării căutării și nu includ date de identificare directă a persoanei.
(3) Datele dactiloscopice neidentificate trebuie să poată fi recunoscute ca atare.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 13. Date dactiloscopice de referință (3) Datele dactiloscopice neidentificate se marchează distinct și sunt recunoscute ca atare în cadrul sistemului de schimb automatizat și al Registrului de stat dactiloscopic.
Articolul 11. Căutarea automatizată a datelor dactiloscopice (1) În scopul prevenirii, depistării și investigării infracțiunilor, statele membre permit punctelor de contact naționale ale altor state membre și Europol accesul la datele dactiloscopice de referință din bazele lor de date naționale pe care le-au instituit în acest scop, pentru a efectua căutări automatizate prin compararea datelor dactiloscopice de referință. Căutările menționate la primul paragraf se efectuează numai în contextul unor cazuri		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 14. Căutarea automatizată a datelor dactiloscopice (1) În scopul prevenirii, depistării și investigării infracțiunilor, autoritatea competentă de aplicare a legii asigură căutarea automatizată în datele dactiloscopice de referință din Registrul de stat dactiloscopic, la solicitarea punctului național de

individuale și în conformitate cu dreptul intern al statului membru solicitant.			contact al statelor membre ale Uniunii Europene și Europol, în condițiile cadrului normativ în domeniul de cooperare aplicabil. Căutările se realizează prin solicitare automatizată, fără acordarea accesului direct la conținutul Registrului de stat dactiloscopic. (2) Căutările automatizate prevăzute la alin. (1) se efectuează numai în cazuri individuale. În cazul în care autoritatea competentă de aplicare a legii are calitatea de solicitant, inițierea și efectuarea căutărilor se realizează în conformitate cu prezenta lege și normele privind protecția datelor cu caracter personal, iar dacă autoritatea competentă de aplicare a legii are calitatea de solicitat, cererile se examinează și se execută în condițiile prezentei legi și ale cadrului normativ național aplicabil.
(2) Punctul de contact național al statului membru solicitant poate decide să confirme o concordanță între două seturi de date dactiloscopice. Dacă decide să confirme o concordanță între două seturi de date dactiloscopice, acesta informează statul membru solicitat și se asigură că se efectuează o revizuire manuală de către cel puțin un membru calificat al personalului pentru a confirma respectiva concordanță cu datele		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 14. Căutarea automatizată a datelor dactiloscopice (3) Dacă în urma căutării automatizate autoritatea competentă de aplicare a legii primește un rezultat pozitiv („hit”), confirmarea concordanței

dactiloscopice de referință primite de la statul membru solicitat.			dintre seturile de date dactiloscopice se realizează numai după efectuarea unei verificări manuale de cel puțin un membru al personalului calificat, în scopul validării concordanței pe baza datelor dactiloscopice de referință primite. În cazul confirmării concordanței, punctul național de contact informează fără întârziere punctul de contact din statul membru solicitat, potrivit procedurilor stabilite.
Articolul 12. Numerele de referință pentru datele dactiloscopice Numerele de referință pentru datele dactiloscopice reprezintă combinația dintre următoarele: (a) un număr de referință care permite statelor membre, în cazul unei concordanțe, să extragă date suplimentare și alte informații din bazele lor de date menționate la articolul 10 pentru a le furniza unuia, mai multor sau tuturor celorlalte state membre, în conformitate cu articolul 47, sau către Europol, în conformitate cu articolul 49 alineatul (6); (b) un număr de referință care permite Europol, în cazul unei concordanțe, să extragă date suplimentare și alte informații în sensul articolului 48 alineatul (1) din prezentul regulament pentru a le furniza unuia, mai multor sau tuturor statelor membre, în conformitate cu Regulamentul (UE) 2016/794;		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> prevede și completarea <i>Legii nr. 1549/2002 cu privire la înregistrarea dactiloscopică de stat, cu noțiunea „date dactiloscopice de referință”</i>. Articolul 2. Noțiuni principale <i>date dactiloscopice de referință</i>– reprezintă combinația dintre următoarele elemente: a) număr de referință care permite localizarea setului de date dactiloscopice corespunzător în Registrul de stat dactiloscopic, în cazul unei concordanțe, în vederea furnizării ulterioare de date suplimentare potrivit procedurilor legale aplicabile; b) un număr de referință care permite asocierea datelor dactiloscopice cu fluxurile de

(c) un cod care indică statul membru care deține datele dactiloscopice.			schimb de date realizate prin intermediul Europol, în condițiile dreptului Uniunii Europene și ale cadrului normativ național; c) un cod care indică statul care deține datele dactiloscopice. Totodată, prevederile urmează să se regăsească inclusiv în proiectul de modificare a Hotărârii de Guvern nr. 509/2019 pentru aprobarea Regulamentului privind modalitatea de ținere a Registrului de stat dactiloscopic, format de Sistemul informațional automatizat „Registrul de stat dactiloscopic”.
Articolul 13. Principii privind schimbul de date dactiloscopice (1) Statele membre iau măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea datelor dactiloscopice trimise altor state membre sau Europol, inclusiv criptarea acestora. Europol ia măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea datelor dactiloscopice trimise statelor membre, inclusiv criptarea acestora.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 509/2019 pentru aprobarea Regulamentului privind modalitatea de ținere a Registrului de stat dactiloscopic, format de Sistemul informațional automatizat „Registrul de stat dactiloscopic”</i>.
(2) Fiecare stat membru și Europol se asigură că datele dactiloscopice pe care le transmite sunt de o calitate suficientă pentru a permite compararea automatizată. Comisia stabilește, prin intermediul actelor de punere în aplicare, un standard minim de calitate care să permită compararea datelor dactiloscopice.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 509/2019 pentru aprobarea Regulamentului privind modalitatea de ținere a Registrului de stat dactiloscopic, format de Sistemul informațional</i>

			<i>automatizat „Registrul de stat dactiloscopic”.</i> Partea a doua a normei (referitoare la stabilirea de către Comisia Europeană, prin acte de punere în aplicare, a standardului minim de calitate are caracter instituțional specific Uniunii Europene.
(3) Datele dactiloscopice se digitalizează și se transmit către celelalte state membre sau către Europol în conformitate cu standardele europene sau internaționale. Comisia adoptă acte de punere în aplicare prin care precizează standardele europene sau internaționale relevante care trebuie utilizate de statele membre și Europol pentru schimbul de date dactiloscopice.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 509/2019 pentru aprobarea Regulamentului privind modalitatea de ținere a Registrului de stat dactiloscopic, format de Sistemul informațional automatizat „Registrul de stat dactiloscopic”.</i> Partea a doua a normei (referitoare la stabilirea de către Comisia Europeană, prin acte de punere în aplicare standardelor europene sau internaționale relevante are caracter instituțional specific Uniunii Europene.
(4) Acte de punere în aplicare menționate în alineatele (2) și (3) de la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).		Prevedere UE neaplicabilă	Prevederea reglementează procedura prin care Comisia Europeană adoptă acte de punere în aplicare (procedura de examinare – comitologie). Dispoziția ține de mecanismul decizional intern al Uniunii Europene și nu stabilește norme

			juridice pentru autoritățile naționale.
Articolul 14. Capacități de căutare pentru datele dactiloscopice (1) Fiecare stat membru se asigură că solicitările sale de căutare nu depășesc capacitățile de căutare precizate de statul membru solicitat sau de Europol, pentru a asigura disponibilitatea sistemului și pentru a evita supraîncărcarea sistemului. În același scop, Europol se asigură că solicitările sale de căutare nu depășesc capacitățile de căutare precizate de statul membru solicitat. Statele membre informează celelalte state membre, Comisia, eu-LISA și Europol cu privire la capacitățile lor maxime de căutare pe zi pentru datele dactiloscopice ale persoanelor identificate și neidentificate. Europol informează statele membre, Comisia și eu-LISA cu privire la capacitățile lor maxime de căutare pe zi pentru datele dactiloscopice ale persoanelor identificate și neidentificate. Statele membre sau Europol pot majora în mod temporar sau permanent respectivele capacități de căutare în orice moment, inclusiv în cazul unei urgențe. Dacă un stat membru își majorează respectivele capacități maxime de căutare, notifică celorlalte state membre, Comisiei, eu-LISA și Europol noile capacități maxime de căutare. Dacă Europol își majorează respectivele capacități maxime de căutare, notifică statelor membre, Comisiei și eu-LISA noile capacități maxime de căutare.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 509/2019 pentru aprobarea Regulamentului privind modalitatea de ținere a Registrului de stat dactiloscopic, format de Sistemul informațional automatizat „Registrul de stat dactiloscopic”</i> .
(2) Comisia adoptă acte de punere în aplicare prin care precizează numărul maxim		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui

de candidați acceptați pentru comparație pentru fiecare transmitere și distribuția capacităților de căutare nefolosite între statele membre, în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).			<i>proiect de modificare a Hotărârii de Guvern nr. 509/2019 pentru aprobarea Regulamentului privind modalitatea de ținere a Registrului de stat dactiloscopic, format de Sistemul informațional automatizat „Registrul de stat dactiloscopic”.</i>
Articolul 15. Norme privind solicitările și răspunsurile referitoare la datele dactiloscopice (1) O solicitare de căutare automatizată de date dactiloscopice include numai informațiile următoare: (a) codul statului membru solicitant; (b) data și ora solicitării și numărul solicitării; (c) datele dactiloscopice de referință.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 509/2019 pentru aprobarea Regulamentului privind modalitatea de ținere a Registrului de stat dactiloscopic, format de Sistemul informațional automatizat „Registrul de stat dactiloscopic”.</i>
(2) Un răspuns la o solicitare astfel cum este menționată la alineatul (1) conține numai informațiile următoare: (a) o precizare din care să reiasă dacă a existat una sau au existat mai multe concordanțe sau dacă nu a existat nicio concordanță; (b) data și ora solicitării și numărul solicitării; (c) data și ora răspunsului și numărul răspunsului; (d) codul statului membru solicitant și cel al statului membru solicitat; (e) numerele de referință ale datelor dactiloscopice din statul membru solicitant și din statul membru solicitat; (f) datele dactiloscopice între care s-a stabilit o concordanță.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 509/2019 pentru aprobarea Regulamentului privind modalitatea de ținere a Registrului de stat dactiloscopic, format de Sistemul informațional automatizat „Registrul de stat dactiloscopic”.</i>

(3) Statele membre se asigură că solicitările menționate la alineatul (1) de la prezentul articol sunt corelate cu notificările transmise în temeiul articolului 74. Notificările respective se reproduc în manualul practic menționat la articolul 79.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Hotărârii de Guvern nr. 509/2019 pentru aprobarea Regulamentului privind modalitatea de ținere a Registrului de stat dactiloscopic, format de Sistemul informațional automatizat „Registrul de stat dactiloscopic”</i>.
Articolul 16. Căutarea automatizată a datelor privind înmatricularea vehiculelor (1) În scopul prevenirii, depistării și investigării infracțiunilor, statele membre permit punctelor de contact naționale ale altor state membre și Europol accesul la următoarele date naționale privind înmatricularea vehiculelor, pentru a efectua căutări automatizate în cazuri individuale: (a) datele referitoare la proprietar sau la deținătorul vehiculului; (b) datele referitoare la vehicul.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 15. Căutarea automatizată a datelor privind vehicule (1) În scopul prevenirii, depistării și investigării infracțiunilor, punctul național de contact asigură disponibilitatea datelor din Registrul de stat al vehiculelor pentru efectuarea căutărilor automatizate, la solicitarea punctelor naționale de contact ale statelor membre ale Uniunii Europene și Europol, privind: a) date referitoare la proprietarul sau posesorul vehiculului; b) date referitoare la vehicul; c) date referitoare la vehicule radiate din evidență, precum și piesele componente ale acestuia consemnate cu număr de identificare.

(2) Căutările menționate la alineatul (1) se efectuează doar prin utilizarea următoarelor date: (a) un număr complet de șasiu; (b) un număr complet de înmatriculare; sau (c) datele referitoare la proprietarul sau deținătorul vehiculului, în cazul în care acest lucru este autorizat de dreptul intern al statului membru solicitat.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 15. Căutarea automatizată a datelor privind vehicule (2) Căutările menționate la alin. (1) se efectuează exclusiv prin utilizarea: a) unui număr de șasiu (VIN) complet; b) unui număr de înmatriculare complet; c) unui număr de motor; d) în măsura în care legislația națională a statului solicitat permite, date referitoare la proprietarul ori posesorul vehiculului, în condițiile alin. (3).
(3) Căutările menționate la alineatul (1) efectuate cu datele referitoare la proprietarul sau deținătorul vehiculului se efectuează numai în cazul persoanelor suspectate sau condamnate. În scopul acestor căutări, se utilizează toate datele de identificare următoare: (a) în cazul în care proprietarul sau deținătorul vehiculului este o persoană fizică: (i) prenumele persoanei fizice; (ii) numele de familie al persoanei fizice; și (iii) data nașterii persoanei fizice; (b) în cazul în care proprietarul sau deținătorul vehiculului este o persoană juridică, denumirea persoanei juridice respective.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 15. Căutarea automatizată a datelor privind vehicule (3) Căutările efectuate în baza datelor referitoare la proprietarul sau deținătorul vehiculului sunt permise exclusiv în privința persoanelor care au calitatea de bănuțit, învinuit, inculpat sau condamnat. În acest scop se utilizează: a) pentru persoanele fizice: numele, prenumele și data nașterii;

			b) pentru persoanele juridice: denumirea oficială.
(4) Căutările menționate la alineatul (1) pot fi efectuate numai în conformitate cu dreptul intern al statului membru solicitant.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 15. Căutarea automatizată a datelor privind vehicule (2) Căutările menționate la alin. (1) se efectuează exclusiv prin utilizarea: d) în măsura în care legislația națională a statului solicitat permite, date referitoare la proprietarul ori posesorul vehiculului, în condițiile alin. (3).
Articolul 17. Principii de căutare automatizată a datelor privind înmatricularea vehiculelor (1) Pentru căutarea automatizată a datelor privind înmatricularea vehiculelor, statele membre utilizează Sistemul de informații european privind vehiculele și permisele de conducere (Eucaris).		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Regulamentului cu privire la registrul de stat al vehiculelor, aprobat prin Hotărârea de Guvern nr. 1047/1999.</i>
(2) Informațiile schimbate prin Eucaris se transmit într-o formă criptată.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Regulamentului cu privire la registrul de stat al vehiculelor, aprobat prin Hotărârea de Guvern nr. 1047/1999.</i>
(3) Comisia adoptă acte de punere în aplicare prin care precizează elementele datelor privind înmatricularea vehiculelor care pot face obiectul schimburilor și procedura tehnică prin care Eucaris poate		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Regulamentului cu privire la registrul de stat al vehiculelor, aprobat prin</i>

accesa bazele de date ale statelor membre. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).			<i>Hotărârea de Guvern nr. 1047/1999.</i> Partea a doua a normei conferă Comisiei Europene competența de a adopta acte de punere în aplicare privind elementele datelor de înmatriculare a vehiculelor și procedura tehnică de acces prin EUCARIS.
Articolul 18. Păstrarea înregistrărilor (1) Fiecare stat membru păstrează înregistrări ale interogărilor efectuate de personalul autorităților sale competente, autorizat în mod corespunzător să facă schimb de date privind înmatricularea vehiculelor, precum și înregistrări ale interogărilor solicitate de alte state membre. Europol păstrează înregistrări ale interogărilor efectuate de personalul său autorizat în mod corespunzător. Fiecare stat membru și Europol păstrează înregistrări ale tuturor operațiunilor de prelucrare de date privind înmatricularea vehiculelor. În aceste înregistrări se includ următoarele informații: (a) dacă un stat membru sau Europol a lansat solicitarea de interogare; dacă un stat membru a lansat solicitarea de interogare, se indică statul membru în cauză; (b) data și ora solicitării; (c) data și ora răspunsului; (d) bazele de date naționale către care a fost trimisă o solicitare de interogare; (e) bazele de date naționale care au oferit un răspuns pozitiv.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 45. Norme speciale privind transmiterea automatizată și neautomatizată (1) Punctul național de contact se asigură că orice transmitere și primire neautomatizată de date cu caracter personal, efectuată de autoritatea care administrează fișierul și care efectuează interogarea, este supusă unei proceduri de înregistrare. Evidența respectivă cuprinde cel puțin următoarele informații: a) temeiul și scopul furnizării datelor; b) datele cu caracter personal transmise; c) data efectuării transmiterii; d) denumirea sau codul de identificare al autorității care efectuează căutarea și care administrează fișierul.

			(2) În cazul interogărilor automatizate de date privind profilurile ADN, datele dactiloscopice și datele de înmatriculare a vehiculelor, precum și al comparațiilor automatizate de profiluri ADN neidentificate, se aplică următoarele reguli: a) interogările și comparațiile automatizate de date se efectuează exclusiv de către autoritatea competentă de aplicare a legii, care au drepturi pentru acces și operare. Lista persoanelor autorizate să efectueze căutări sau comparații automatizate se pune la dispoziția autorității naționale de supraveghere competente și, la solicitare, autorităților competente ale statelor participante la schimbul de date; b) punctul național de contact asigură înregistrarea transmiterii și primirii datelor între autoritatea care administrează fișierul și care efectuează căutarea, inclusiv indicarea existenței sau lipsei unui rezultat pozitiv („hit”/„no hit”). Înregistrarea cuprinde cel puțin: datele furnizate, data și ora furnizării și denumirea sau codul de identificare al autorității care efectuează căutarea și care administrează fișierul.

(2) Înregistrările menționate la alineatul (1) sunt utilizate numai pentru colectarea de statistici, pentru monitorizarea protecției datelor, inclusiv verificarea admisibilității unei interogări și a legalității prelucrării datelor, precum și pentru asigurarea securității și integrității datelor. Respectivile înregistrări se protejează prin măsuri corespunzătoare împotriva accesului neautorizat și se șterg după o perioadă de trei ani de la data la care au fost create. Dacă înregistrările sunt însă necesare pentru desfășurarea unor proceduri de monitorizare deja inițiate, acestea se șterg în momentul în care nu mai sunt necesare pentru procedurile de monitorizare.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 45. Norme speciale privind transmiterea automatizată și neautomatizată (4) La cererea autorităților competente în domeniul protecției datelor din statele membre în cauză, autoritatea competentă de aplicare a legii comunică datele înregistrate, în cel mult patru săptămâni de la data primirii cererii. Datele înregistrate pot fi utilizate exclusiv în următoarele scopuri: a) monitorizarea respectării cerințelor de protecție a datelor cu caracter personal; b) asigurarea securității datelor. (5) Datele înregistrate sunt protejate prin aplicarea de măsuri tehnice și organizatorice împotriva utilizării neautorizate și a oricăror forme de utilizare incorectă și se păstrează pe o perioadă de 3 ani, cu excepția înregistrărilor prevăzute la art. 40, care se păstrează pentru termenul special stabilit de acestea. La expirarea termenului de păstrare, datele înregistrate se șterg imediat.
(3) În scopul monitorizării protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Regulamentului cu</i>

prelucrării datelor, operatorii de date au acces la înregistrări pentru automonitorizarea menționată la articolul 55.			<i>privire la registrul de stat al vehiculelor, aprobat prin Hotărârea de Guvern nr. 1047/1999.</i>
Articolul 19. Date de referință privind imaginile faciale (1) Statele membre asigură disponibilitatea datelor de referință privind imaginile faciale ale suspecților, ale persoanelor condamnate și, în cazul în care dreptul intern permite acest lucru, ale victimelor, din bazele lor de date naționale create pentru prevenirea, depistarea și investigarea infracțiunilor.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 18. Date de referință privind imaginile faciale (1) Autoritatea competentă de aplicare a legii asigură disponibilitatea datelor de referință privind imaginile faciale ale bănuțiților, învinuiților, inculpaților, condamnaților, și, după caz, ale victimelor din baza de date națională, în măsura în care cadrul normativ național permite acest lucru.
(2) Datele de referință privind imaginile faciale nu conțin niciun fel de date suplimentare care să permită identificarea directă a unei persoane.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 18. Date de referință privind imaginile faciale (2) Datele de referință privind imaginile faciale puse la dispoziție de autoritatea competentă de aplicare a legii nu conțin date care permit identificarea directă a persoanei.
(3) Imaginile faciale neidentificate sunt recunoscute ca atare.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 18. Date de referință privind imaginile faciale

			(3) Imaginile faciale neidentificate, colectate în cursul investigării infracțiunilor, sunt marcate și recunoscute ca atare în bazele de date naționale, precum și în cadrul schimbului automatizat de date.
Articolul 20. Căutarea automatizată a imaginilor faciale (1) În scopul prevenirii, depistării și investigării infracțiunilor pentru care este prevăzută o pedeapsă maximă cu închisoarea de cel puțin un an în temeiul dreptului statului membru solicitant, statele membre permit punctelor de contact naționale ale altor state membre și Europol accesul la datele de referință privind imaginile faciale stocate în bazele lor de date naționale, pentru a efectua căutări automatizate. Căutările menționate la primul paragraf se efectuează numai în contextul unor cazuri individuale și în conformitate cu dreptul intern al statului membru solicitant. Crearea de profiluri astfel cum este menționată la articolul 11 alineatul (3) din Directiva (UE) 2016/680 este interzisă.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 19. Căutarea automatizată a imaginilor faciale (1) Pentru infracțiunile pentru care legislația statului solicitant prevede o pedeapsă privativă de libertate mai mare de 1 an, autoritatea competentă de aplicare a legii asigură schimbul automatizat de date și accesul statelor membre și EUROPOL la datele de referință privind imaginile faciale din baza de date națională, în vederea efectuării căutărilor automatizate. (2) Căutările menționate la alin. (1) se efectuează exclusiv în cazuri individuale. În cazul în care autoritatea competentă de aplicare a legii are calitatea de solicitant, căutarea imaginilor faciale se realizează în condițiile prezentei legi și ale cadrului normativ național aplicabil. (3) Se interzice utilizarea căutării automatizate ale imaginilor faciale pentru crearea

			de profiluri care pot duce la discriminarea persoanelor. (4) Prelucrarea datelor biometrice și a altor categorii speciale de date cu caracter personal în cadrul căutării automatizate a imaginilor faciale este permisă numai în măsura strict necesară și proporțională pentru scopurile prevăzute de prezenta lege, cu respectarea garanțiilor stabilite de aceasta și de legislația aplicabilă în domeniul protecției datelor cu caracter personal.
(2) Punctul de contact național al statului membru solicitant poate decide să confirme o concordanță între două imagini faciale. Dacă decide să confirme o concordanță între două imagini faciale, acesta informează statul membru solicitat și se asigură că se efectuează o revizuire manuală a listei de către cel puțin un membru calificat al personalului pentru a confirma această concordanță cu datele de referință privind imaginile faciale primite de la statul membru solicitat.			<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 19. Căutarea automatizată a imaginilor faciale (5) În cazul în care autoritatea competentă de aplicare a legii a Republicii Moldova are calitatea de autoritate solicitată și, în urma căutării automatizate, obține un rezultat pozitiv („hit”), confirmarea concordanței dintre două imagini faciale se realizează numai după efectuarea unei verificări manuale de către cel puțin un membru al personalului calificat, în scopul validării concordanței pe baza datelor de referință primite. În cazul confirmării concordanței, punctul național de contact al Republicii

			Moldova informează fără întârziere punctul național de contact al statului membru solicitant, potrivit procedurilor stabilite.
Articolul 21. Numerele de referință pentru imaginile faciale Numerele de referință pentru imaginile faciale reprezintă combinația dintre următoarele: (a) un număr de referință care permite statelor membre, în cazul unei concordanțe, să extragă date suplimentare și alte informații din bazele lor de date menționate la articolul 19 pentru a le furniza unuia, mai multor sau tuturor celorlalte state membre, în conformitate cu articolul 47, sau către Europol, în conformitate cu articolul 49 alineatul (6); (b) un număr de referință care permite Europol, în cazul unei concordanțe, să extragă date suplimentare și alte informații în sensul articolului 48 alineatul (1) din prezentul regulament pentru a le furniza unuia, mai multor sau tuturor statelor membre, în conformitate cu Regulamentul (UE) 2016/794; (c) un cod care indică statul membru care deține imaginile faciale.		Parțial compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 17. Numerele de referință pentru imaginile faciale Numărul de referință pentru imaginile faciale reprezintă combinația dintre următoarele elemente: a) un identificator unic care permite autorităților competente ale Republicii Moldova, în cazul unei concordanțe, să extragă date de bază și informații suplimentare din baza de date națională, în vederea furnizării acestora statelor membre ale Uniunii Europene, Europol sau prin intermediul canalelor INTERPOL, în condițiile procedurilor legale; b) după caz, un identificator tehnic care permite corelarea schimbului realizat prin intermediul Europol și INTERPOL; c) un cod de țară care indică Republica Moldova sau alt stat membru al Europol sau INTERPOL, după caz, statul membru al Uniunii Europene care deține imaginile faciale respective;

			d) un indicator care arată statutul identificat sau neidentificat al imaginii faciale. Prevederea urmează, inclusiv, să se regăsească în <i>noul proiect de Hotărâre a Guvernului pentru stabilirea unei baze de date privind imaginile faciale</i>.
Articolul 22. Principii privind schimbul de imagini faciale (1) Statele membre iau măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea imaginilor faciale trimise altor state membre sau Europol, inclusiv criptarea acestora. Europol ia măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea imaginilor faciale trimise statelor membre, inclusiv criptarea acestora.		Parțial compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 19. Căutarea automatizată a imaginilor faciale (7) În cadrul sistemului de căutare și schimb automatizat de date privind imaginile faciale, transmiterea și primirea datelor de referință privind imaginile faciale se realizează cu asigurarea confidențialității și integrității acestora, inclusiv prin utilizarea criptării și a altor măsuri tehnice și organizatorice, în condițiile prezentei legi. (8) Standardele, cerințele tehnice, parametrii tehnici, evidența operațiunilor, profilurile de acces, rolurile tehnice și procedurile de funcționare a mecanismului de căutare și schimb automatizat de date privind imaginile faciale se stabilesc de Guvern.

			Prevederea urmează, inclusiv, să se regăsească în <i>noul proiect de Hotărâre a Guvernului pentru stabilirea unei baze de date privind imaginile faciale.</i>
(2) Fiecare stat membru și Europol se asigură că imaginile faciale pe care le transmite sunt de o calitate suficientă pentru a permite compararea automatizată. Comisia stabilește, prin intermediul actelor de punere în aplicare, un standard minim de calitate care să permită compararea imaginilor faciale. Dacă raportul menționat la articolul 80 alineatul (7) indică un risc ridicat de concordanțe false, Comisia revizuieste actele de punere în aplicare respective.		Parțial compatibil O parte din prevedere UE este neaplicabilă se referă la activitatea Comisiei	Prevederea reglementează adoptarea de către Comisia Europeană a actelor de punere în aplicare privind standardele tehnice pentru schimbul de imagini faciale și procedura aferentă, în cadrul mecanismului de comitologie. Dispozițiile privesc standarde tehnice și procese instituționale ale Uniunii Europene și nu stabilesc norme juridice pentru autoritățile naționale. Obligația națională de a transmite numai imagini de calitate suficientă să fie introdusă în <i>HG privind baza de date cu imagini faciale</i>, standardul tehnic concret va urma actele UE de punere în aplicare sau, până la acelea, standardele europene/internaționale aplicabile.
(3) Comisia adoptă acte de punere în aplicare prin care precizează standardele relevante europene sau internaționale pentru schimbul de imagini faciale care trebuie să fie utilizate de statele membre și de Europol.		Parțial compatibil O parte din prevedere UE este neaplicabilă	<i>HG privind baza de date cu imagini faciale</i> va prevedea expres că digitalizarea, transmiterea și compararea imaginilor faciale se fac conform standardelor europene sau internaționale relevante. În schimb, dispoziția privind

		se referă la activitatea Comisiei	adoptarea actelor de punere în aplicare de către Comisie nu se transpune ca normă națională, dar se tratează ca prevedere UE neaplicabilă Prevederea reglementează adoptarea de către Comisia Europeană a actelor de punere în aplicare privind standardele tehnice pentru schimbul de imagini faciale și procedura aferentă, în cadrul mecanismului de comitologie. Dispozițiile privesc standarde tehnice și procese instituționale ale Uniunii Europene și nu stabilesc norme juridice pentru autoritățile naționale.
(4) Actele de punere în aplicare menționate în alineatele (2) și (3) de la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).		Prevedere UE neaplicabilă	Prevederea reglementează adoptarea de către Comisia Europeană a actelor de punere în aplicare privind standardele tehnice pentru schimbul de imagini faciale și procedura aferentă, în cadrul mecanismului de comitologie. Dispozițiile privesc standarde tehnice și procese instituționale ale Uniunii Europene și nu stabilesc norme juridice pentru autoritățile naționale.
Articolul 23. Capacitățile de căutare a imaginilor faciale (1) Fiecare stat membru se asigură că solicitările sale de căutare nu depășesc		Prevedere UE netranspusă	Această prevedere urmează a fi reglementată în <i>HG privind baza de date cu imagini faciale</i>, unde să fie prevăzute capacitățile zilnice

capacitățile de căutare specificate de statul membru solicitat sau de Europol pentru a asigura disponibilitatea sistemului și pentru a evita supraîncărcarea sistemului. În același scop, Europol se asigură că solicitările sale de căutare nu depășesc capacitățile de căutare specificate de statul membru solicitat. Statele membre informează celelalte state membre, Comisia, eu-LISA și Europol cu privire la capacitățile lor maxime de căutare pe zi pentru schimburile de imagini faciale identificate sau neidentificate. Europol informează statele membre, Comisia și eu-LISA cu privire la capacitățile sale maxime de căutare pe zi pentru schimburile de imagini faciale identificate și neidentificate. Statele membre sau Europol pot majora în mod temporar sau permanent respectivele capacități de căutare în orice moment, inclusiv în cazul unei urgențe. Dacă un stat membru își majorează respectivele capacități maxime de căutare, notifică celorlalte state membre, Comisiei, eu-LISA și Europol noile capacități maxime de căutare. Dacă Europol își majorează respectivele capacități maxime de căutare, notifică statelor membre, Comisiei și eu-LISA noile capacități maxime de căutare.			pentru imagini faciale identificate/neidentificate, procedura de majorare temporară/permanentă și fluxul de notificare către statele membre, Comisie, eu-LISA și Europol.
(2) Comisia adoptă acte de punere în aplicare prin care precizează numărul maxim de candidați acceptați pentru comparație pentru fiecare transmitere și distribuția capacităților de căutare nefolosite între statele membre, în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).		Incompatibil	Dispoziția conferă Comisiei Europene competența de a adopta acte de punere în aplicare privind parametrii tehnici ai capacităților de căutare a imaginilor faciale și distribuția acestora între statele membre. Aceasta vizează gestionarea tehnică a infrastructurii UE și nu stabilește

			norme juridice pentru autoritățile naționale. În <i>HG privind baza de date cu imagini faciale</i> urmează a fi inserată o clauză de conformare tehnică la parametrii stabiliți la nivelul UE, fără a reproduce competența Comisiei.
Articolul 24. Norme privind solicitările și răspunsurile referitoare la imaginile faciale (1) O solicitare de căutare automatizată de imagini faciale include numai informațiile următoare: (a) codul statului membru solicitant; (b) data și ora solicitării și numărul solicitării; (c) datele de referință privind imaginile faciale.		Prevedere UE netranspusă	Prevederea urmează să se regăsească în noul <i>proiect de Hotărâre a Guvernului pentru stabilirea unei baze de date privind imaginile faciale</i>.
(2) Un răspuns la o solicitare astfel cum este menționată la alineatul (1) conține numai informațiile următoare: (a) o precizare din care să reiasă dacă a existat una sau au existat mai multe concordanțe sau dacă nu a existat nicio concordanță; (b) data și ora solicitării și numărul solicitării; (c) data și ora răspunsului și numărul răspunsului; (d) codul statului membru solicitant și cel al statului membru solicitat; (e) numerele de referință ale imaginilor faciale din statul membru solicitant și din statul membru solicitat;		Prevedere UE netranspusă	Prevederea urmează să se regăsească în noul <i>proiect de Hotărâre a Guvernului pentru stabilirea unei baze de date privind imaginile faciale</i>.

(f) imaginile faciale între care s-a stabilit o concordanță.			
(3) Statele membre se asigură că solicitările menționate la alineatul (1) de la prezentul articol sunt corelate cu notificările transmise în temeiul articolului 74. Notificările respective se reproduc în manualul practic menționat la articolul 79.		Parțial compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 53. Notificări (1) Punctul național de contact notifică Agenția eu-LISA lista autorităților competente, autorizate să utilizeze Routerul ori să aibă acces la acesta în scopul căutării și schimbului de profiluri ADN, date dactiloscopice și imagini faciale. (2) Orice modificare privind lista autorităților naționale autorizate să acceseze Routerul, precum și actualizarea profilurilor de acces ale membrilor personalului autorizat, se comunică Agenției eu-LISA fără întârzieri nejustificate. (3) Autoritatea competentă informează, prin intermediul punctului național de contact, celelalte state membre ale Uniunii Europene, Comisia Europeană, Agenția eu-LISA și Europol privind conținutul Registrului de stat al datelor genetice, precum și condițiile tehnice și juridice stabilite pentru efectuarea căutărilor automatizate de profiluri ADN. (4) Autoritatea competentă informează, prin intermediul

		punctului național de contact, celelalte state membre ale Uniunii Europene, Comisia Europeană, Agenția eu-LISA și Europol privind conținutul Registrului de stat dactiloscopic, precum și condițiile tehnice și juridice stabilite pentru efectuarea căutărilor automatizate de date dactiloscopice. (5) Autoritatea competentă informează, prin intermediul punctului național de contact, celelalte state membre ale Uniunii Europene, Comisia Europeană, Agenția eu-LISA și Europol privind conținutul bazei de date naționale privind imaginile faciale, precum și condițiile tehnice și juridice stabilite pentru efectuarea căutărilor automatizate de date ale imaginilor faciale. (6) În vederea participării la schimbul automatizat de evidențe ale poliției, autoritatea competentă informează, prin intermediul punctului național de contact, celelalte state membre ale Uniunii Europene, Comisia Europeană, Agenția eu-LISA și Europol informații privind conținutul registrelor naționale de evidențe ale poliției, sursele de date utilizate pentru stabilirea acestora și criteriile stabilite pentru

			căutările automatizate prin sistemul EPRIS. (7) Punctul unic de contact notifică oficial Comisia Europeană, Agenția eu-LISA și Europol identitatea și datele de legătură ale punctelor naționale de contact desemnate conform art. 6 și utilizează lista centralizată a punctelor naționale de contact, gestionată de Comisia Europeană, pentru coordonarea operativă a schimbului de date. Prevederea urmează să se regăsească în noul <i>proiect de Hotărâre a Guvernului pentru stabilirea unei baze de date privind imaginile faciale</i>.
Articolul 25. Evidențe ale poliției (1) Statele membre pot participa la schimbul automatizat de evidențe ale poliției. În scopul unor astfel de schimburi, statele membre participante asigură accesul la registrele naționale de evidențe ale poliției care conțin seturi de date biografice ale suspectilor și ale persoanelor condamnate din bazele lor de date naționale create pentru prevenirea, depistarea și investigarea infracțiunilor. Respectivetele seturi de date conțin numai următoarele date, în măsura în care sunt disponibile: (a) prenumele; (b) numele; (c) pseudonimul sau pseudonimele și numele utilizat sau numele utilizate anterior;		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 20. Evidențe ale poliției (1) Autoritatea competentă de aplicare a legii asigură schimbul automatizat de evidențe ale poliției și accesul la Registrul informației criminalistice și criminologice, care conțin date biografice despre bănuți, învinuiți, inculpați și condamnați, extrase din bazele de date naționale. (2) Seturile de date puse la dispoziție prin intermediul

(d) data nașterii; (e) cetățenia sau cetățeniile; (f) țara nașterii; (g) genul. (2) Datele menționate la alineatul (1) literele (a), (b), și (c) trebuie să fie pseudonimizate.			infrastructurii EPRIS conțin următoarele informații: a) prenumele și numele; b) pseudonimul sau pseudonimele și numele utilizat anterior; c) data, luna și anul nașterii; d) cetățenia sau cetățeniile; e) țara nașterii; f) genul. (3) În cadrul schimbului automatizat, datele prevăzute la alin. (2) lit. (a) - (c) se transmit obligatoriu sub formă pseudonimizată, prin utilizarea unor serii alfanumerice care împiedică identificarea directă a persoanei în etapa de căutare.
Articolul 26. Căutarea automatizată în registrele naționale de evidențe ale poliției În scopul prevenirii, depistării și investigării infracțiunilor pentru care este prevăzută o pedeapsă maximă cu închisoarea de cel puțin un an în temeiul dreptului statului membru solicitant, statele membre participante la schimbul automatizat de evidențe ale poliției permit punctelor de contact naționale ale altor state membre participante și Europol accesul la datele din registrele naționale de evidențe ale poliției, pentru a efectua căutări automatizate. Căutările menționate la primul paragraf se efectuează numai în contextul unor cazuri individuale și în conformitate cu dreptul intern al statului membru solicitant.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 21. Căutarea automatizată în Registrul informației criminalistice și criminologice (1) În scopul prevenirii, depistării și investigării infracțiunilor pentru care legea statului solicitant prevede o pedeapsă cu închisoarea mai mare de un an, autoritatea competentă de aplicare a legii asigură schimbul automatizat de evidențe și accesul la datele din registrele naționale de evidențe ale poliției statelor membre și Europol.

			(2) Căutările automatizate în evidențele poliției se efectuează exclusiv în evidențele persoanelor reținute, bănuților, învinuiților, și persoanelor condamnate, precum și în alte evidențe prevăzute în mod expres de actele normative aplicabile care reglementează sistemele informaționale polițienești, iar accesul automatizat la datele privind victimele și martorii este permis numai în cazurile de căutare a persoanelor dispărute fără veste, de identificare a cadavrelor, a persoanelor implicate în situații de urgență sau pericol pentru viață ori sănătate, precum și în alte situații prevăzute expres de lege.
Articolul 27. Numerele de referință pentru evidențele poliției Numerele de referință pentru evidențele poliției reprezintă combinația dintre următoarele: (a) un număr de referință care permite statelor membre, în cazul unei concordanțe, să extragă date biografice și alte informații din registrele de evidențe ale poliției menționate la articolul 25 pentru a le furniza unuia, mai multor sau tuturor celorlalte state membre, în conformitate cu articolul 44; (b) un cod care indică statul membru care deține evidențele poliției.		Prevedere UE netranspusă	Prevederea urmează să se regăsească în reglementările interne privind evidența poliției
Articolul 28. Norme privind solicitările și răspunsurile referitoare la evidențele poliției		Prevedere UE netranspusă	Prevederea urmează să se regăsească în reglementările interne privind evidența poliției

(1) O solicitare de căutare automatizată în registrele naționale de evidențe ale poliției include numai informațiile următoare: (a) codul statului membru solicitant; (b) data și ora solicitării și numărul solicitării; (c) datele menționate la articolul 25, în măsura în care sunt disponibile.			
(2) Un răspuns la o solicitare astfel cum este menționată la alineatul (1) conține numai informațiile următoare: (a) o precizare a numărului de concordanțe; (b) data și ora solicitării și numărul solicitării; (c) data și ora răspunsului și numărul răspunsului; (d) codul statului membru solicitant și cel al statului membru solicitat; (e) numerele de referință ale evidențelor poliției din statele membre solicitate.		Prevedere UE netranspusă	Prevederea urmează să se regăsească în reglementările interne privind evidența poliției
(3) Statele membre se asigură că solicitările menționate la alineatul (1) de la prezentul articol sunt corelate cu notificările transmise în temeiul articolului 74. Notificările respective se reproduc în manualul practic menționat la articolul 79.		Prevedere UE netranspusă	Prevederea urmează să se regăsească în reglementările interne privind evidența poliției
Articolul 29. Persoane dispărute și rămășițe umane neidentificate (1) Dacă o autoritate națională are competențe în acest sens în temeiul unor măsuri legislative naționale, astfel cum se menționează la alineatul (2), aceasta poate efectua căutări automatizate prin intermediul cadrului Prüm II exclusiv în scopul:		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 22. Căutarea persoanelor dispărute fără veste, identificarea cadavrelor sau a părților acestuia (1) Autoritatea competentă de aplicare a legii este împuternicită

(a) căutării persoanelor dispărute în contextul anchetelor penale sau din motive umanitare; (b) identificării de rămășițe umane.			să efectueze căutări automatizate în evidențele altor state, prin mecanismele prevăzute de prezenta lege exclusiv în scopul: a) căutării persoanelor dispărute fără veste în contextul cauzelor penale sau din motive umanitare, cum ar fi identificarea victimelor catastrofelor naturale, accidentelor aviatice, feroviare sau în alte situații de urgență, unde viața ori sănătatea persoanei este în pericol; b) identificării cadavrelor și a părților acestuia.
(2) Statele membre care doresc să facă uz de posibilitatea prevăzută la alineatul (1) desemnează, prin intermediul unor măsuri legislative naționale, autoritățile naționale competente în scopurile prevăzute în astfel de măsuri și stabilesc proceduri, condiții și criterii, inclusiv motivele umanitare pentru care este permis să se efectueze căutări automatizate ale persoanelor dispărute astfel cum se menționează la alineatul (1) litera (a).		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 22. Căutarea persoanelor dispărute fără veste, identificarea cadavrelor sau a părților acestuia (2) Desemnarea autorității competente, procedura, condițiile, criteriile și cazurile umanitare în care este permisă efectuarea căutărilor automatizate ale persoanelor dispărute fără veste, a cadavrelor și a părților acestuia, precum și garanțiile privind protecția datelor cu caracter personal se stabilesc prin Hotărâre de Guvern.
Articolul 30. Puncte de contact naționale		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i>

Fiecare stat membru desemnează unul sau mai multe puncte de contact naționale în sensul articolelor 6, 11, 16, 20 și 26.		Articolul 6. Punctul unic de contact și atribuțiile acestuia (1) Se desemnează în calitate de punct unic de contact pentru cooperarea polițienească internațională subdiviziunea specializată în cooperare polițienească internațională din subordinea Inspectoratului General al Poliției al Ministerului Afacerilor Interne. (2) Punctul unic de contact asigură cooperarea cu punctele naționale de contact desemnate prin hotărâre de Guvern, din cadrul autorităților competente naționale, pe următoarele domenii: a) profiluri ADN; b) date dactiloscopice; c) date referitoare la mijloace de transport, inclusiv autovehicule anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale; d) imagini faciale; e) evidențe polițienești, inclusiv date nominale privind persoanele urmărite, dispărute sau implicate în activități infracționale; f) date care nu privesc persoanele și informații operative; g) date cu caracter personal prelucrate în contextul

			evenimentelor majore cu dimensiune transfrontalieră și de prevenire a infracțiunilor cu caracter terorist; h) date privind documentele de călătorie, vizele, titlurile de valoare, inclusiv cele declarate furate, pierdute, nevalidate sau false. i) date privind permisele de conducere. (7) Organizarea, funcțiile și modul de funcționare a punctului unic de contact și a punctelor naționale de contact pe domeniile prevăzute la alin. (2), se stabilesc prin hotărâre de Guvern.
Articolul 31. Măsuri de punere în aplicare Comisia adoptă acte de punere în aplicare prin care precizează modalitățile tehnice pentru statele membre cu privire la procedurile prevăzute la articolele 6, 11, 16, 20 și 26. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).		Prevedere UE neaplicabilă	Prevederile acestui articol se referă la competențele executive ale Comisiei Europene și la mecanismul de comitologie (procedura de examinare conform Regulamentului 182/2011) pentru adoptarea specificațiilor tehnice. În calitate de stat non-membru UE, Republica Moldova nu are capacitatea juridică de a transpune delegarea de competențe către Comisia Europeană sau procedurile de vot în cadrul comitetelor europene. Totuși, proiectul de hotărâre asigură conformitatea tehnică prin precizarea că procedurile de interogare, formatul răspunsurilor

			și normele de comparare „sunt stabilite în conformitate cu actele de punere în aplicare și specificațiile tehnice adoptate la nivelul Uniunii Europene”.
Articolul 32. Disponibilitatea schimbului automatizat de date la nivel național (1) Statele membre iau toate măsurile necesare pentru a asigura posibilitatea efectuării de căutări automatizate de profiluri ADN, de date dactiloscopice, de anumite date privind înmatricularea vehiculelor, de imagini faciale și de evidențe ale poliției timp de 24 de ore pe zi, 7 zile pe săptămână.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 9. Schimbul de date la nivel național, inclusiv automatizat (1) Autoritatea competentă de aplicare a legii adoptă și implementează măsurile tehnice și organizatorice necesare pentru a garanta disponibilitatea permanentă a sistemelor informatice și funcționalitatea interogărilor automatizate pentru categoriile de date prevăzute de prezenta lege, asigurând un regim de funcționare continuă (24 de ore din 24, 7 zile pe săptămână).
(2) Punctele de contact naționale se informează reciproc și informează Comisia, eu-LISA și Europol, fără întârziere, cu privire la orice indisponibilitate a schimbului automatizat de date, inclusiv, după caz, cu privire la orice defecțiuni tehnice care cauzează această indisponibilitate. Punctele de contact naționale convin, în conformitate cu dreptul aplicabil al Uniunii și cu dreptul intern aplicabil, asupra unor modalități alternative temporare pentru schimbul de informații, care să fie utilizate în		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 9. Schimbul de date la nivel național, inclusiv automatizat (2) Interoperabilitatea vizează: a) schimbul de date între registrele naționale; b) integrarea cu sistemele informatice europene și internaționale;

cazurile în care schimbul automatizat de date nu este disponibil.			c) utilizarea standardelor comune. (3) Autoritatea competentă de aplicare a legii are obligația de a informa, prin canalele securizate și fără întârziere, punctele de contact ale statelor membre ale Uniunii Europene, Comisia Europeană, agențiile eu-LISA și Europol cu privire la orice indisponibilitate a sistemelor de schimb automatizat de date, indicând natura defecțiunilor tehnice și durata estimată a remedierii acestora.
(3) Atunci când schimbul automatizat de date nu este disponibil, punctele de contact naționale se asigură că acesta este restabilit, prin orice mijloace necesare fără întârziere.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 9. Schimbul de date la nivel național, inclusiv automatizat (4) Dacă schimbul automatizat de date este indisponibil, punctul național de contact stabilește modalități alternative temporare pentru schimbul de informații, utilizând canalele de comunicare securizate de rezervă.
Articolul 33. Justificarea prelucrării datelor (1) Fiecare stat membru păstrează o evidență a justificărilor pentru interogările pe care le efectuează autoritățile sale competente. Europol păstrează o evidență a justificărilor pentru interogările pe care le efectuează.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 42. Evidența prelucrării datelor (1) Autoritățile competente și punctul național de contact păstrează evidența tuturor solicitărilor efectuate în bazele de

			date naționale și internaționale în condițiile prezentei legi.
(2) Justificările menționate la alineatul (1) cuprind: (a) scopul interogării, inclusiv o referire la cazul sau ancheta respectivă, și, după caz, infracțiunea specifică; (b) o precizare dacă interogarea se referă la un suspect sau la o persoană condamnată pentru comiterea unei infracțiuni, la o victimă a unei infracțiuni, la o persoană dispărută sau la rămășițe umane neidentificate; (c) o precizare dacă interogarea vizează identificarea unei persoane sau obținerea mai multor date cu privire la o persoană cunoscută.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 42. Evidența prelucrării datelor (2) Evidența menționată la alin. (1) cuprinde următoarele elemente obligatorii: a) scopul solicitării, inclusiv menționarea cauzei penale, după caz, calificarea juridică a faptei; b) statutul persoanei (bănuț, învinuit, condamnat, victimă, persoană dispărută fără veste, cadavru sau părțile acestuia); c) tipul solicitării (identificarea unei persoane sau obținere de date suplimentare cu privire la o persoană cunoscută).
(3) Justificările menționate la alineatul (1) de la prezentul articol trebuie să poată fi urmărite până la înregistrările menționate la articolele 18, 40 și 45. Respectivile justificări se pot utiliza numai pentru a evalua în ce măsură căutările sunt proporționale și necesare în scopul prevenirii, depistării sau investigării unei infracțiuni, pentru monitorizarea protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, precum și pentru asigurarea securității și integrității datelor. Respectivile justificări se protejează prin măsuri corespunzătoare împotriva accesului neautorizat și se șterg		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 42. Evidența prelucrării datelor (3) Evidența este corelată cu înregistrările (log-urile) privind operațiunile de prelucrare a datelor și sunt utilizate exclusiv pentru: a) evaluarea proporționalității și necesității căutărilor; b) controlul legalității prelucrării datelor. (4) Regimul de securitate, acces, păstrare și ștergere a

după o perioadă de trei ani de la data la care au fost create. Dacă înregistrările sunt însă necesare pentru desfășurarea unor proceduri de monitorizare aflate în curs, acestea se șterg odată ce nu mai sunt necesare pentru procedurile de monitorizare.			evidenței se stabilesc prin hotărâre de Guvern. Articolul 43. Înregistrarea operațiunilor de acces și schimb de date (4) Înregistrările sunt supuse măsurilor tehnice și organizatorice de securitate, fiind păstrate pentru o perioadă de trei ani de la data creării. (5) În cazul în care înregistrările sunt necesare pentru desfășurarea unor proceduri de monitorizare, audit sau control aflate în curs, acestea se păstrează până la finalizarea procedurilor respective. (6) Operatorii de date au acces la înregistrările prevăzute în prezentul articol pentru activități de monitorizare internă, în cooperare, după caz, cu autoritatea de supraveghere competentă.
(4) Pentru evaluarea proporționalității și a necesității căutărilor în scopul prevenirii, depistării și investigării unei infracțiuni sau al monitorizării protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, operatorii de date au acces la respectivele justificări pentru automonitorizarea menționată la articolul 55.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 48. Automonitorizarea (1) Autoritatea competentă ia măsurile necesare pentru a respecta prezenta lege și cooperează cu Centrul Național pentru Protecția Datelor cu Caracter Personal.

			(2) Operatorii de date implementează măsuri tehnice și organizatorice pentru a monitoriza respectarea prezentei legi, inclusiv prin verificarea anuală a înregistrărilor (log-urilor), activităților de prelucrare, conform cerințelor de audit stabilite de legislația națională și cooperează cu Centrul Național pentru Protecția Datelor cu Caracter Personal pentru a asigura transparența prelucrărilor.
Articolul 34. Utilizarea formatului universal pentru mesaje (1) În măsura în care este posibil, la dezvoltarea routerului menționat la articolul 35 din prezentul regulament și a Sistemului european de inventariere a evidențelor poliției (EPRIS) se utilizează standardul privind formatul universal pentru mesaje (UMF) instituit prin articolul 38 din Regulamentul (UE) 2019/818.	<i>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</i> Anexa nr.1 Punctul 50. 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, ASP, CTC-EJ), în etapa de operare a sistemelor proprii.	Compatibil	
(2) Orice schimb automatizat de date în conformitate cu prezentul regulament utilizează standardul UMF, în măsura în care este posibil.	<i>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</i> Anexa nr.2 Punctul 12. În vederea asigurării unui schimb internațional de date și informații structurat și a interoperabilității tehnice, PNC-	Compatibil	

	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.		
Articolul 35. Routerul (1) Se creează un router cu scopul de a facilita stabilirea de conexiuni între statele membre și între statele membre și Europol pentru interogarea, extragerea și evaluarea datelor biometrice și pentru extragerea datelor alfanumerice în conformitate cu prezentul regulament.	<i>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</i> Anexa nr.1 Punctul 43. În scopul facilitării stabilirii de conexiuni între Republica Moldova, statele membre ale Uniunii Europene și Europol, PUC utilizează Router-ul ca punct central de legătură pentru interogarea, extragerea și evaluarea automatizată a datelor biometrice, precum și pentru extragerea datelor alfanumerice.	Compatibil	
(2) Routerul este alcătuit din următoarele elemente: (a) o infrastructură centrală, care include un instrument de căutare ce permite interogarea simultană a bazelor de date naționale menționate la articolele 5, 10 și 19, precum și a datelor Europol; (b) un canal securizat de comunicații între infrastructura centrală, autoritățile competente autorizate să utilizeze routerul în temeiul articolului 36 și Europol;	<i>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</i> Anexa nr.1 Punctul 44. Arhitectura tehnică utilizată de PUC prin intermediul Router-ului este alcătuită din următoarele elemente componente, administrate tehnic de către Punctul Național de Contact tehnic:	Compatibil	

(c) o infrastructură de comunicații securizată între infrastructura centrală și portalul european de căutare, instituit prin articolul 6 din Regulamentul (UE) 2019/817 și articolul 6 din Regulamentul (UE) 2019/818, în sensul articolului 39.	44.1. infrastructura centrală, care include un instrument de căutare ce permite interogarea simultană a bazelor de date naționale și a datelor gestionate de Europol; 44.2. canalul securizat de comunicații între infrastructura centrală și autoritățile competente; 44.3. infrastructura de comunicații securizată care asigură legătura cu ESP.		
Articolul 36. Utilizarea routerului Utilizarea routerului este rezervată autorităților competente ale statelor membre care sunt autorizate să acceseze și să facă schimbul de profiluri ADN, de date dactiloscopice și de imagini faciale în conformitate cu prezentul regulament, precum și Europol, în conformitate cu prezentul regulament și cu Regulamentul (UE) 2016/794.	<i>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</i> Anexa nr.1 Punctul 45. 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 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.	Compatibil	
Articolul 37. Procedură (1) Autoritățile competente autorizate să utilizeze routerul în temeiul articolului 36 sau Europol solicită o interogare prin transmiterea de date biometrice către router. Routerul trimite solicitarea de interogare către bazele de date ale tuturor sau anumitor state membre și către datele Europol simultan cu datele transmise de utilizator în conformitate cu drepturile sale de acces.	<i>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</i> Anexa nr.1 Punctul 52. PUC este responsabil de lansarea 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	Compatibil	

	considera că datele privind un bănuț sau o victimă a unei infracțiuni de terorism ori a unei alte infracțiuni grave sunt stocate în respectivul registru.		
(2) La primirea unei solicitări de interogare din partea routerului, fiecare stat membru solicitat lansează o interogare în bazele lor de date în mod automatizat și fără întârziere. La primirea unei solicitări de interogare din partea routerului, Europol lansează o interogare în datele Europol în mod automatizat și fără întârziere.	<i>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</i> Anexa nr.1 Punctul 53. La primirea unei solicitări de interogare din partea Router-ului, PUC, în calitate de autoritate a statului solicitat, asigură lansarea interogării în bazele de date naționale în mod automatizat și fără întârziere.	Compatibil	
(3) Toate concordanțele rezultate în urma interogărilor astfel cum se menționează la alineatul (2) sunt trimise înapoi în mod automatizat routerului. Statul membru solicitant este informat în mod automat în cazul în care nu există nicio concordanță.	<i>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</i> Anexa nr.1 Punctul 55. 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.	Compatibil	
(4) Dacă statul membru solicitant decide astfel și dacă acest lucru este aplicabil, routerul clasifică răspunsurile comparând datele biometrice utilizate pentru interogare și datele biometrice furnizate în răspunsurile din partea statului membru solicitat sau a statelor membre solicitate sau ale Europol.	<i>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</i> Anexa nr.1 Punctul 56. În cazul în care PUC, în calitate de autoritate a statului solicitant, solicită clasificarea rezultatelor și dacă	Compatibil	

	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.		
(5) Routerul returnează utilizatorului routerului lista datelor biometrice între care s-a stabilit o concordanță și clasificarea acestora.	<i>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</i> Anexa nr.1 Punctul 57. Router-ul returnează PUC, în calitate de utilizator al Router-ului, lista datelor biometrice între care s-a stabilit o concordanță și clasificarea acestora.	Compatibil	
(6) Comisia adoptă acte de punere în aplicare prin care precizează procedura tehnică pentru interogarea de către router a bazelor de date ale statelor membre și a datelor Europol, formatul în care routerul răspunde la astfel de interogări și normele tehnice pentru compararea și clasificarea corespondenței dintre datele biometrice. Respectivle acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).		Prevedere UE neaplicabilă	Prevederile acestui alineat vizează atribuții de reglementare ale Comisiei Europene și mecanisme de comitologie (procedura de examinare) care sunt specifice raporturilor juridice interne ale Uniunii Europene și nu pot fi transpuse în legislația națională a unui stat terț. Cu toate acestea, proiectul de hotărâre asigură alinierea tehnică deplină prin punctul 52 din Anexa nr. 1, care stabilește că: „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”. În plus, punctul 18 din Anexa nr. 2 impune Punctelor Naționale de Contact obligația de a actualiza periodic aceste formate în conformitate cu specificațiile europene, asigurând astfel interoperabilitatea continuă a sistemelor naționale cu Router-ul UE.
Articolul 38. Verificarea calității Statul membru solicitat verifică calitatea datelor transmise printr-o procedură automatizată. Statul membru solicitat informează, fără întârziere, statul membru solicitant prin intermediul routerului atunci când datele sunt necorespunzătoare pentru a se efectua o comparare automatizată.	<i>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</i> Anexa nr.1 Punctul 60. 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. Punctul 61. 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.	Compatibil	
Articolul 39. Interoperabilitatea dintre router și registrul comun de date de	<i>Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de</i>	Compatibil	

identitate în scopul accesului autorităților de aplicare a legii (1) Atunci când autoritățile desemnate, astfel cum sunt definite la articolul 4 punctul 20 din Regulamentul (UE) 2019/817 și la articolul 4 punctul 20 din Regulamentul (UE) 2019/818 sunt autorizate să utilizeze routerul în temeiul articolului 36 din prezentul regulament, acestea pot lansa o interogare în bazele de date ale statelor membre și în datele Europol simultan cu o interogare în registrul comun de date de identitate, instituit prin articolul 17 din Regulamentul (UE) 2019/817 și articolul 17 din Regulamentul (UE) 2019/818, cu condiția să fie îndeplinite condițiile relevante prevăzute de dreptul Uniunii și ca interogarea să fie lansată în conformitate cu drepturile lor de acces. În acest scop, routerul efectuează interogări în registrul comun de date de identitate prin intermediul portalului european de căutare.	<i>Contact în scopul schimbului de date și informații</i> Anexa nr.1 Punctul 52. PUC este responsabil de lansarea 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 bănuț sau o victimă a unei infracțiuni de terorism ori a unei alte infracțiuni grave sunt stocate în respectivul registru.		
(2) Interogările în registrul comun de date de identitate în scopul asigurării respectării legii se efectuează în conformitate cu articolul 22 din Regulamentul (UE) 2019/817 și cu articolul 22 din Regulamentul (UE) 2019/818. Orice rezultat al unor astfel de interogări se transmite prin intermediul portalului european de căutare.	<i>Proiectul Hotărârii de Guvern cu privire la înstituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații</i> Anexa nr.1 Punctul 54. 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.	Compatibil	
Interogările simultane în bazele de date ale statelor membre și în datele Europol și în registrul comun de date de identitate sunt lansate numai atunci când există motive	<i>Proiectul Hotărârii de Guvern cu privire la înstituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de</i>	Compatibil	

rezonabile să se considere că date privind un suspect, un autor sau o victimă a unei infracțiuni de terorism sau a unei alte infracțiuni grave, astfel cum sunt definite la articolul 4 punctele 21 și 22 din Regulamentul (UE) 2019/817 și, respectiv, la articolul 4 punctele 21 și 22 din Regulamentul (UE) 2019/818, sunt stocate în registrul comun de date de identitate.	Contact în scopul schimbului de date și informații Anexa nr.1 Punctul 52. PUC este responsabil de lansarea 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 bănuț sau o victimă a unei infracțiuni de terorism ori a unei alte infracțiuni grave sunt stocate în respectivul registru.		
Articolul 40. Păstrarea înregistrărilor (1) eu-LISA păstrează înregistrări ale tuturor operațiunilor de prelucrare de date efectuate în router. Respectivele înregistrări includ următoarele informații: (a) dacă un stat membru sau Europol a lansat solicitarea de interogare; dacă un stat membru a lansat solicitarea de interogare, se indică statul membru în cauză; (b) data și ora solicitării; (c) data și ora răspunsului; (d) bazele de date naționale sau datele Europol către care a fost trimisă o solicitare de interogare; (e) bazele de date naționale sau datele Europol care au oferit un răspuns; (f) după caz, faptul că a existat o interogare simultană în registrul comun de date de identitate.		Compatibil	Proiectul de lege privind cooperarea polițienească internațională Articolul 43. Înregistrarea operațiunilor de acces și schimb de date (1) Punctul național de contact asigură păstrarea la nivel național a înregistrărilor tuturor operațiunilor de acces și schimb de date, automatizate sau neautomatizate, efectuate prin Router, EUCARIS, sistemul EPRIS sau prin alte sisteme informaționale utilizate în aplicarea prezentei legi. (2) Înregistrările prevăzute la alin. (1) conțin cel puțin următoarele informații: a) entitatea care a inițiat solicitarea (autoritate competentă, stat membru al Uniunii Europene sau Europol);

			b) data și ora transmiterii solicitării; c) data și ora transmiterii răspunsului; d) bazele de date naționale sau bazele de date ale Europol către care a fost adresată solicitarea; e) bazele de date care au furnizat răspunsul; f) mențiunea existenței unei solicitări simultane, după caz.
(2) Fiecare stat membru păstrează înregistrări ale interogărilor efectuate de personalul autorităților sale competente autorizat în mod corespunzător să utilizeze routerul, precum și înregistrări ale interogărilor solicitate de alte state membre. Europol păstrează înregistrări ale interogărilor efectuate de personalul său autorizat în mod corespunzător.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 43. Înregistrarea operațiunilor de acces și schimb de date (1) Punctul național de contact asigură păstrarea la nivel național a înregistrărilor tuturor operațiunilor de acces și schimb de date, automatizate sau neautomatizate, efectuate prin Router, EUCARIS, sistemul EPRIS sau prin alte sisteme informaționale utilizate în aplicarea prezentei legi.
(3) Înregistrările menționate la alineatele (1) și (2) sunt utilizate numai pentru colectarea de statistici și pentru monitorizarea protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, precum și pentru asigurarea securității și integrității datelor. Respectivele înregistrări se protejează prin măsuri corespunzătoare împotriva accesului		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 43. Înregistrarea operațiunilor de acces și schimb de date (3) Înregistrările sunt utilizate pentru elaborarea de date statistice, pentru verificarea

neautorizat și se șterg după o perioadă de trei ani de la data la care au fost create. Dacă înregistrările sunt însă necesare pentru desfășurarea unor proceduri de monitorizare deja inițiate, acestea se șterg în momentul în care nu mai sunt necesare pentru procedurile de monitorizare.			legalității accesului și prelucrării datelor, precum și pentru asigurarea trasabilității operațiunilor efectuate. (4) Înregistrările sunt supuse măsurilor tehnice și organizatorice de securitate, fiind păstrate pentru o perioadă de trei ani de la data creării. (5) În cazul în care înregistrările sunt necesare pentru desfășurarea unor proceduri de monitorizare, audit sau control aflate în curs, acestea se păstrează până la finalizarea procedurilor respective.
(4) În scopul monitorizării protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, operatorii de date au acces la înregistrări pentru automonitorizarea menționată la articolul 55.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 48. Automonitorizarea (1) Autoritatea competentă ia măsurile necesare pentru a respecta prezenta lege și cooperează cu Centrul Național pentru Protecția Datelor cu Caracter Personal. (2) Operatorii de date implementează măsuri tehnice și organizatorice pentru a monitoriza respectarea prezentei legi, inclusiv prin verificarea anuală a înregistrărilor (log-urilor), activităților de prelucrare, conform cerințelor de audit stabilite de legislația națională și

			cooperează cu Centrul Național pentru Protecția Datelor cu Caracter Personal pentru a asigura transparența prelucrărilor.
Articolul 41. Proceduri de notificare în cazul imposibilității tehnice de a utiliza routerul (1) În cazul în care este imposibil din punct de vedere tehnic să se utilizeze routerul pentru a efectua interogări în una sau mai multe baze de date naționale sau în datele Europol din cauza unei defecțiuni a routerului, eu-LISA notifică utilizatorii routerului menționați la articolul 36, în mod automatizat. eu-LISA ia măsuri corespunzătoare pentru a soluționa imposibilitatea tehnică de a utiliza routerul.		Prevedere UE neaplicabilă	Prevederile acestui alineat sunt neaplicabile deoarece reglementează obligații executive și procedurale directe pentru agenția eu-LISA (notificarea automată a utilizatorilor și adoptarea măsurilor de remediere), aspecte care țin exclusiv de dreptul Uniunii Europene și nu pot fi impuse prin acte normative ale Republicii Moldova. Totuși, mecanismul de reacție al statului la recepționarea unei astfel de notificări este asigurat prin punctul 11.1 din Anexa nr. 1, care stabilește atribuția Punctului Unic de Contact (PUC) de a monitoriza disponibilitatea sistemelor, precum și prin punctul 75 din Anexa nr. 1, care definește rolul PUC de coordonator operativ în caz de indisponibilitate tehnică externă.
(2) În cazul în care este imposibil din punct de vedere tehnic să se utilizeze routerul pentru a efectua interogări în una sau mai multe baze de date naționale din cauza unei defecțiuni a infrastructurii naționale dintr-un stat membru, statul membru respectiv notifică acest lucru celorlalte state membre, Comisiei, eu-LISA și	<i>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</i> Anexa nr.1	Compatibil	

Europol în mod automatizat. Statul membru vizat ia măsuri corespunzătoare fără întârziere pentru a soluționa imposibilitatea tehnică de a utiliza routerul.	Punctul 86. 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. Punctul 87. 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. Punctul 88. PNC sau autoritățile competente deținătoare ale infrastructurii afectate întreprind imediat toate măsurile tehnice și organizatorice necesare pentru restabilirea funcționării sistemelor informatice.		
(3) În cazul în care este imposibil din punct de vedere tehnic să se utilizeze routerul pentru a efectua interogări în datele Europol din cauza unei defecțiuni a infrastructurii Europol, Europol notifică acest lucru statelor membre, Comisiei și eu-LISA în mod automatizat. Europol ia măsuri corespunzătoare fără întârziere pentru a soluționa imposibilitatea tehnică de a utiliza routerul.		Prevedere UE neaplicabilă	Prevederile sunt neaplicabile sub aspectul impunerii unei sarcini de notificare agenției Europol, legislația națională neavând competența de a reglementa activitatea agențiilor Uniunii Europene. Sub aspect funcțional, procedura de recepționare a acestor notificări de către autoritățile naționale este integral transpusă la punctul 65 din Anexa

			nr. 1, care stipulează explicit că: „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”.
Articolul 42. EPRIS (1) Se stabilește Sistemul european de inventariere a evidențelor poliției (EPRIS). Pentru căutarea automatizată în registrele naționale ale evidențelor poliției menționate la articolul 26, statele membre și Europol utilizează EPRIS.	<i>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</i> Anexa nr.1 Punctul 46. Pentru căutarea de date în registrele naționale ale evidențelor poliției, PUC utilizează sistemul EPRIS ca infrastructură tehnică de interconectare.	Compatibil	
(2) EPRIS este alcătuit din: (a) o infrastructură descentralizată în statele membre, care include un instrument de căutare care permite interogarea simultană a registrelor naționale ale evidențelor poliției, pe baza bazelor de date naționale; (b) o infrastructură centrală, care sprijină instrumentul de căutare care permite interogarea simultană a registrelor naționale ale evidențelor poliției; (c) un canal de comunicații securizat între infrastructura centrală, statele membre și Europol.	<i>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</i> Anexa nr.1 Punctul 47. Sistemul EPRIS, pus la dispoziția PUC de către STI al MAI, include: 47.1. o infrastructură descentralizată instalată la nivel național; 47.2. un instrument de căutare ce permite interogarea simultană a registrelor naționale; 47.3. un instrument de căutare ce permite interogarea simultană a registrelor naționale;	Compatibil	

	47.3. un canal de comunicații securizat.		
Articolul 43. Utilizarea EPRIS (1) În scopul efectuării de căutări în registrele naționale ale evidențelor poliției prin intermediul EPRIS, se utilizează cel puțin două dintre următoarele seturi de date: (a) prenumele; (b) numele; (c) data nașterii.	<i>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</i> Anexa nr.1 Punctul 64. În scopul efectuării de căutări în registrele naționale ale evidențelor poliției prin intermediul EPRIS, în vederea identificării persoanelor urmărite, dispărute sau implicate în activități infracționale, PUC utilizează cel puțin două dintre următoarele date: 64.1. prenumele; 64.2. numele; 64.3. data nașterii.	Compatibil	
(2) În cazul în care sunt disponibile, se pot utiliza, de asemenea, următoarele seturi de date: (a) pseudonimul sau pseudonimele și numele utilizat sau numele utilizate anterior; (b) cetățenia sau cetățeniile; (c) țara nașterii; (d) genul.	<i>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</i> Anexa nr.1 Punctul 65. În cazul în care sunt disponibile, se pot utiliza suplimentar următoarele date: 65.1. pseudonimul (sau numele utilizat anterior); 65.2. cetățenia; 65.3. țara nașterii; 65.4. genul.	Compatibil	
(3) Datele menționate la alineatul (1) literele (a) și (b) și la alineatul (2) litera (a), trebuie să fie pseudonimizate.	<i>Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de</i>	Compatibil	

	<i>Contact în scopul schimbului de date și informații</i> Anexa nr.1 Punctul 66. 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.		
Articolul 44. Procedură (1) Atunci când statele membre sau Europol solicită o interogare, transmit datele menționate la articolul 43. EPRIS transmite cererea de interogare către registrele naționale ale evidențelor poliției din statele membre cu datele transmise de statul membru solicitant sau Europol și în conformitate cu prezentul regulament.		Prevedere UE neaplicabilă	Prevederea referitoare la faptul că „EPRIS transmite cererea de interogare” este neaplicabilă sub aspectul reglementării naționale, deoarece vizează autonomia tehnică și algoritmi de funcționare ai infrastructurii europene (gestionată de Europol), asupra căreia Republica Moldova nu are competență de legiferare.
(2) La primirea solicitării de interogare din partea EPRIS, fiecare stat membru solicitat lansează, în mod automatizat și fără întârziere, o interogare în registrul său național de evidențe ale poliției.	<i>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</i> Anexa nr.1 Punctul 67. 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.	Compatibil	
(3) Toate concordanțele rezultate în urma interogărilor menționate la alineatul (1) în registrele de evidențe ale poliției ale fiecărui stat membru solicitat sunt trimise înapoi în mod automatizat către EPRIS.	<i>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</i>	Compatibil	

	Anexa nr.1 Punctul 68. Toate concordanțele rezultate urmare a interogărilor în registrul național de evidențe ale poliției sunt trimise înapoi, în mod automatizat, către EPRIS.		
(4) Lista concordanțelor este returnată statului membru solicitant sau Europol de către EPRIS, în mod automatizat. Lista concordanțelor precizează calitatea concordanței și statul membru sau statele membre ale căror registre de evidențe ale poliției conțin date care au condus la concordanța sau la concordanțele respective.	<i>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</i> Anexa nr.1 Punctul 69. Lista concordanțelor, precizând calitatea acestora și statul deținător al datelor, este returnată către PUC de către sistemul EPRIS în mod automatizat.	Compatibil	
(5) La primirea listei de concordanțe, statul membru solicitant decide cu privire la concordanțele pentru care este necesară o acțiune ulterioară și trimite, prin intermediul SIENA, statului membru solicitat sau statelor membre solicitate o solicitare motivată de acțiune ulterioară cuprinzând datele menționate la articolele 25 și 27, precum și eventuale informații suplimentare relevante. Statul membru solicitat sau statele membre solicitate prelucrează aceste solicitări fără întârziere pentru a decide dacă partajează datele stocate în baza lor de date.	<i>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</i> Anexa nr.1 Punctul 70. 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.	Compatibil	
(6) Comisia adoptă acte de punere în aplicare prin care precizează procedura tehnică pentru efectuarea de către EPRIS a interogării registrelor de evidențe ale poliției statelor membre, precum și formatul răspunsurilor și numărul maxim al acestora. Respectivile acte de punere în aplicare se		Prevedere UE neaplicabilă	Prevederile acestui alineat vizează competențele executive ale Comisiei Europene și mecanismele de comitologie (procedura de examinare conform Regulamentului 182/2011) pentru stabilirea detaliilor tehnice ale

adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).			sistemului EPRIS. Republica Moldova, în calitate de stat non-membru UE, nu are capacitatea juridică de a transpune delegarea de competențe către Comisia Europeană sau procedurile de vot în cadrul comitetelor europene.
Articolul 45. Păstrarea înregistrărilor (1) Fiecare stat membru participant și Europol păstrează înregistrări ale tuturor operațiunilor de prelucrare de date efectuate în EPRIS. În aceste înregistrări se includ următoarele informații: (a) dacă un stat membru sau Europol a lansat solicitarea de interogare; dacă un stat membru a lansat solicitarea de interogare, se indică statul membru în cauză; (b) data și ora solicitării; (c) data și ora răspunsului; (d) bazele de date naționale către care a fost trimisă o solicitare de interogare; (e) bazele de date naționale care au oferit un răspuns.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 43. Înregistrarea operațiunilor de acces și schimb de date (1) Punctul național de contact asigură păstrarea la nivel național a înregistrărilor tuturor operațiunilor de acces și schimb de date, automatizate sau neautomatizate, efectuate prin Router, EUCARIS, sistemul EPRIS sau prin alte sisteme informaționale utilizate în aplicarea prezentei legi. (2) Înregistrările prevăzute la alin. (1) conțin cel puțin următoarele informații: a) entitatea care a inițiat solicitarea (autoritate competentă, stat membru al Uniunii Europene sau Europol); b) data și ora transmiterii solicitării; c) data și ora transmiterii răspunsului;

			d) bazele de date naționale sau bazele de date ale Europol către care a fost adresată solicitarea; e) bazele de date care au furnizat răspunsul; f) mențiunea existenței unei solicitări simultane, după caz.
(2) Fiecare stat membru participant păstrează înregistrări ale interogărilor efectuate de personalul autorităților sale competente autorizat în mod corespunzător să utilizeze EPRIS. Europol păstrează înregistrări ale solicitărilor de interogări pe care le efectuează personalul său autorizat în mod corespunzător.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 43. Înregistrarea operațiunilor de acces și schimb de date (1) Punctul național de contact asigură păstrarea la nivel național a înregistrărilor tuturor operațiunilor de acces și schimb de date, automatizate sau neautomatizate, efectuate prin Router, EUCARIS, sistemul EPRIS sau prin alte sisteme informaționale utilizate în aplicarea prezentei legi.
(3) Înregistrările menționate la alineatele (1) și (2) pot fi folosite numai pentru colectarea de statistici și pentru monitorizarea protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, precum și pentru asigurarea securității și integrității datelor. Respectivile înregistrări se protejează prin măsuri corespunzătoare împotriva accesului neautorizat și se șterg după o perioadă de trei ani de la data la care au fost create. Dacă înregistrările sunt însă necesare pentru desfășurarea unor proceduri de monitorizare		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 43. Înregistrarea operațiunilor de acces și schimb de date (3) Înregistrările sunt utilizate pentru elaborarea de date statistice, pentru verificarea legalității accesului și prelucrării datelor, precum și pentru asigurarea trasabilității operațiunilor efectuate.

deja inițiate, acestea se șterg în momentul în care nu mai sunt necesare pentru procedurile de monitorizare.			(4) Înregistrările sunt supuse măsurilor tehnice și organizatorice de securitate, fiind păstrate pentru o perioadă de trei ani de la data creării. (5) În cazul în care înregistrările sunt necesare pentru desfășurarea unor proceduri de monitorizare, audit sau control aflate în curs, acestea se păstrează până la finalizarea procedurilor respective.
(4) În scopul monitorizării protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, operatorii de date au acces la înregistrări pentru automonitorizarea menționată la articolul 55.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 43. Înregistrarea operațiunilor de acces și schimb de date (6) Operatorii de date au acces la înregistrările prevăzute în prezentul articol pentru activități de monitorizare internă, în cooperare, după caz, cu autoritatea de supraveghere competentă.
Articolul 46. Proceduri de notificare în cazul imposibilității tehnice de a utiliza EPRIS (1) În cazul în care este imposibil din punct de vedere tehnic să se utilizeze EPRIS pentru a efectua interogări în unul sau mai multe registre naționale de evidențe ale poliției din cauza unei defecțiuni a infrastructurii Europol, Europol notifică acest lucru statelor membre în mod automatizat. Europol ia măsuri fără întârziere pentru a soluționa imposibilitatea tehnică de a utiliza EPRIS.		Prevedere UE neaplicabilă	Prevederile acestui alineat sunt incompatibile sub aspectul reglementării naționale, deoarece impun obligații de notificare automatizată și sarcini de remediere tehnică direct în sarcina agenției Europol. Legislația Republicii Moldova nu are competența de a reglementa atribuțiile executive, procedurile interne sau termenele de

			intervenție ale agențiilor Uniunii Europene.
(2) În cazul în care este imposibil din punct de vedere tehnic să se utilizeze EPRIS pentru a efectua interogări în unul sau mai multe registre de evidențe ale poliției din cauza unei defecțiuni a infrastructurii naționale dintr-un stat membru, statul membru respectiv notifică acest lucru celorlalte state membre, Comisiei și Europol în mod automatizat. Statele membre iau măsuri fără întârziere pentru a soluționa imposibilitatea tehnică de a utiliza EPRIS.	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 Anexa nr.1 Punctul 72. 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.	Compatibil	
Articolul 47. Schimbul de date de bază (1) Un set de date de bază se returnează prin router în termen de 48 de ore de la îndeplinirea cumulativă a condițiilor următoare: (a) procedurile menționate la articolul 6, 11 sau 20 indică o concordanță între datele utilizate pentru căutare și datele stocate în baza de date a statului membru solicitat sau a statelor membre solicitate; (b) concordanța menționată la litera (a) de la prezentul alineat a fost confirmată manual de către un membru calificat din statul membru solicitant astfel cum se menționează la articolul 6 alineatul (6), articolul 11 alineatul (2) și articolul 20 alineatul (2) sau, în cazul profilurilor ADN menționate la articolul 6 alineatul (7), de către statul membru solicitat; (c) a fost transmisă o descriere a faptelor și a fost indicată infracțiunea subiacentă, utilizând tabelul comun al categoriilor de		Compatibil	Proiectul de lege privind cooperarea polițienească internațională Articolul 44. Schimbul de date în urma unei concordanțe (1) Setul de date de bază se transmite prin intermediul Routerului în termen de cel mult 48 de ore de la îndeplinirea cumulativă a următoarelor condiții: a) procedurile de căutare a profilurilor ADN, a datelor dactiloscopice sau a imaginilor faciale indică o concordanță între datele utilizate pentru căutare și datele stocate în bazele de date naționale sau ale statelor membre ale Uniunii Europene; b) concordanța menționată la lit. a) a fost confirmată manual de către un membru calificat al

infracțiuni prevăzut într-un act de punere în aplicare care urmează să fie adoptat în temeiul articolului 11b alineatul (1) litera (a) din Decizia-cadru 2009/315/JAI, de către statul membru solicitant sau, în cazul profilurilor ADN menționate la articolul 6 alineatul (7), de către statul membru solicitat, pentru a evalua proporționalitatea cererii, inclusiv gravitatea infracțiunii pentru care a fost efectuată o căutare, în conformitate cu dreptul intern al statului membru care furnizează setul de date de bază.			autorității desemnate, în calitate de stat solicitant, conform prevederilor art. 11 alin. (7), art. 14 alin. (3), art. 19 alin. (5); c) a fost transmisă o descriere a faptelor și a fost indicată infracțiunea predicat, utilizând tabelul comun al categoriilor de infracțiuni stabilit la nivelul Uniunii Europene, de către autoritatea solicitantă sau, în cazul profilurilor ADN prevăzute la art. 11 alin. (7), de către statul membru solicitat, în scopul evaluării proporționalității cererii și a gravității infracțiunii, în conformitate cu cadrul normativ al statului care furnizează datele.
(2) Atunci când, în temeiul dreptului său intern, un stat membru poate transmite un set de date de bază numai după obținerea unei autorizații judiciare, statul membru respectiv se poate abate de la termenele stabilite la alineatul (1) în măsura în care acest lucru este necesar pentru obținerea unei astfel de autorizații.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 44. Schimbul de date în urma unei concordanțe (2) În cazul în care, conform cadrului normativ național, autoritatea competentă de aplicare a legii poate transmite un set de date de bază numai în temeiul unei autorizații judiciare, punctele naționale de contact pot devia de la termenul de 48 de ore prevăzut la alin. (1) strict pentru perioada necesară obținerii acestei autorizații.

(3) Setul de date de bază menționat la alineatul (1) de la prezentul articol se returnează de către statul membru solicitat sau, în cazul profilurilor ADN menționate la articolul 6 alineatul (7), de către statul membru solicitant.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 44. Schimbul de date în urma unei concordanțe (3) Setul de date de bază prevăzut la alin. (1) este returnat de către autoritatea competentă de aplicare a legii , atunci când are calitatea de stat solicitat, sau de către statul membru solicitant în cazul profilurilor ADN confirmate conform procedurii prevăzute la art. 11 alin. (7).
(4) În cazul în care concordanța confirmată se referă la datele identificate ale unei persoane, setul de date de bază menționat la alineatul (1) conține următoarele date, în măsura în care sunt disponibile: (a) prenumele; (b) numele de familie; (c) pseudonimul sau pseudonimele și numele utilizat sau numele utilizate anterior; (d) data nașterii; (e) cetățenia sau cetățeniile; (f) locul și țara nașterii; (g) genul; (h) data la care și locul unde au fost obținute datele biometrice; (i) infracțiunea pentru care au fost obținute datele biometrice; (j) numărul cauzei penale; (k) autoritatea competentă responsabilă de cauza penală.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 44. Schimbul de date în urma unei concordanțe (4) Atunci când concordanța confirmată vizează datele identificate ale unei persoane, setul de date de bază menționat la alin. (1) transmis de autoritatea competentă de aplicare a legii sau primit de la un stat membru conține următoarele informații: a) numele și prenumele; b) data nașterii; c) pseudonimul sau pseudonimele și numele utilizat anterior; d) cetățenia sau cetățeniile; e) locul și țara nașterii; f) genul;

			g) data și locul obținerii datelor biometrice; h) infracțiunea pentru care au fost obținute datele biometrice; i) numărul dosarului/cauzei penale; j) autoritatea competentă responsabilă de cauza penală.
5) În cazul în care concordanța confirmată se referă la date neidentificate sau urme, setul de date de bază menționat la alineatul (1) conține următoarele date, în măsura în care sunt disponibile: (a) data la care și locul unde au fost obținute datele biometrice; (b) infracțiunea pentru care au fost obținute datele biometrice; (c) numărul cauzei penale; (d) autoritatea competentă responsabilă de cauza penală.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 44. Schimbul de date în urma unei concordanțe (5) În cazul în care concordanța confirmată se referă la date neidentificate sau urme, setul de date de bază menționat la alin. (1) conține următoarele date: a) data și locul când au fost obținute datele biometrice; b) infracțiunea pentru care au fost obținute datele biometrice; c) numărul cauzei penale; d) autoritatea competentă responsabilă de examinarea cauzei penale.
(6) Returnarea datelor de bază de către statul membru solicitat sau, în cazul specific al profilurilor ADN menționate la articolul 6 alineatul (7), de către statul membru solicitant face obiectul unei decizii luate de un factor uman.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 44. Schimbul de date în urma unei concordanțe (6) Decizia de a returna setul de date de bază de către autoritățile competente, în calitate de parte solicitată, sau, în cazul profilurilor ADN prevăzut la art. 11 alin. (7),

			în calitate de parte solicitantă, nu poate fi luată exclusiv prin mijloace automatizate și este supusă verificării și aprobării de către o persoană autorizată.
Articolul 48. Accesul statelor membre la datele biometrice furnizate de țări terțe și stocate de Europol (1) În conformitate cu Regulamentul (UE) 2016/794, statele membre au acces la datele biometrice puse la dispoziția Europol de către țările terțe în sensul articolului 18 alineatul (2) literele (a), (b) și (c) din Regulamentul (UE) 2016/794 și pot efectua căutări prin intermediul routerului.	<i>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</i> Anexa nr.1 Punctul 62. 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 desfășoară în conformitate cu normele Regulamentului (UE) 2016/794 privind Europol.	Compatibil	
(2) În cazul în care o căutare, astfel cum este menționată la alineatul (1), conduce la o concordanță între datele utilizate pentru căutare și datele furnizate de țări terțe și stocate de Europol, acțiunea ulterioară are loc în conformitate cu Regulamentul (UE) 2016/794.	<i>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</i> Anexa nr.1 Punctul 62. 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 desfășoară în conformitate cu	Compatibil	

	normele Regulamentului (UE) 2016/794 privind Europol.		
Articolul 49. Accesul Europol la datele stocate în bazele de date ale statelor membre, utilizând datele furnizate de țări terțe (1) Atunci când este necesar pentru realizarea obiectivelor stabilite la articolul 3 din Regulamentul (UE) 2016/794 și în conformitate cu respectivul regulament și cu prezentul regulament, Europol are acces la datele stocate de statele membre în bazele lor de date naționale și la registrele de evidențe ale poliției.	<i>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</i> Anexa nr.2 Punctul 49. STI al MAI este desemnat în calitate de PNC responsabil pentru domeniul evidențelor poliției cu caracter criminal, contravențional și dactiloscopic, având rolul de a gestiona registrele naționale și de a furniza PUC datele de referință necesare schimbului internațional de date și informații. În exercitarea acestor atribuții, STI asigură operarea tehnică și interconectarea infrastructurii descentralizate a sistemului EPRIS cu sistemele naționale de evidență (Sistemului Informațional Automatizat ”Registrul Informației Criminalistice și Criminologice”), permițând interogarea simultană a registrelor de evidență gestionate de către autoritățile competente din statele membre și Europol.	Compatibil	
(2) Interogările efectuate de Europol utilizând date biometrice drept criteriu de căutare se efectuează utilizând routerul.		Prevedere UE neaplicabilă	Prevederea nu este aplicabilă pentru transpunere în legislația Republicii Moldova, întrucât reglementează drepturi și competențe instituționale ale Europol, agenție a Uniunii Europene, care decurg exclusiv din statutul de stat membru al UE.
(3) Interogările efectuate de Europol utilizând date privind înmatricularea		Prevedere UE neaplicabilă	Prevederea nu este aplicabilă pentru transpunere în legislația Republicii Moldova, întrucât

vehiculelor drept criteriu de căutare se efectuează utilizând Eucaris.			reglementează drepturi și competențe instituționale ale Europol, agenție a Uniunii Europene, care decurg exclusiv din statutul de stat membru al UE.
(4) Interogările efectuate de Europol utilizând date biografice ale suspectilor și ale persoanelor condamnate în conformitate cu prevederile articolului 25 drept criteriu de căutare se efectuează utilizând EPRIS.		Prevedere UE neaplicabilă	Prevederea nu este aplicabilă pentru transpunere în legislația Republicii Moldova, întrucât reglementează drepturi și competențe instituționale ale Europol, agenție a Uniunii Europene, care decurg exclusiv din statutul de stat membru al UE.
(5) Europol efectuează căutările pe baza datelor furnizate de țări terțe în conformitate cu alineatele (1)-(4) de la prezentul articol numai atunci când acest lucru este necesar pentru îndeplinirea atribuțiilor sale în sensul articolului 18 alineatul (2) literele (a) și (c) din Regulamentul (UE) 2016/794.		Prevedere UE neaplicabilă	Prevederea nu este aplicabilă pentru transpunere în legislația Republicii Moldova, întrucât reglementează drepturi și competențe instituționale ale Europol, agenție a Uniunii Europene, care decurg exclusiv din statutul de stat membru al UE.
(6) În cazul în care procedurile menționate la articolele 6, 11 sau 20 indică o concordanță între datele utilizate pentru căutare și datele deținute în baza de date a statului membru solicitat sau a statelor membre solicitate, Europol informează numai statul membru implicat sau statele membre implicate. Statul membru solicitat decide dacă returnează prin router un set de date de bază în termen de 48 de ore de la îndeplinirea cumulativă a condițiilor următoare: (a) concordanța menționată la primul paragraf a fost confirmată manual de către un membru calificat al personalului Europol;		Prevedere UE neaplicabilă	Prevederea nu este aplicabilă pentru transpunere în legislația Republicii Moldova, întrucât reglementează drepturi și competențe instituționale ale Europol, agenție a Uniunii Europene, care decurg exclusiv din statutul de stat membru al UE.

(b) a fost transmisă de către Europol o descriere a faptelor și a fost indicată infracțiunea subiacentă, utilizând tabelul comun al categoriilor de infracțiuni prevăzut într-un act de punere în aplicare care urmează să fie adoptat în temeiul articolului 11b alineatul (1) litera (a) din Decizia-cadru 2009/315/JAI, pentru a evalua proporționalitatea cererii, inclusiv gravitatea infracțiunii pentru care a fost efectuată o căutare, în conformitate cu dreptul intern al statului membru care furnizează setul de date de bază; (c) a fost comunicat numele țării terțe care a furnizat datele; Atunci când, în temeiul dreptului său intern, un stat membru poate transmite un set de date de bază numai după obținerea unei autorizații judiciare, statul membru respectiv se poate abate de la termenele stabilite la al doilea paragraf în măsura în care acest lucru este necesar pentru obținerea unei astfel de autorizații. În cazul în care concordanța confirmată se referă la datele identificate ale unei persoane, setul de date de bază menționat la al doilea paragraf conține următoarele date, în măsura în care sunt disponibile: (a) prenumele; (b) numele de familie; (c) pseudonimul sau pseudonimele și numele utilizat sau numele utilizate anterior; (d) data nașterii; (e) cetățenia sau cetățeniile; (f) locul și țara nașterii; (g) genul;			

(h) data la care și locul unde au fost obținute datele biometrice; (i) infracțiunea pentru care au fost obținute datele biometrice; (j) numărul cauzei penale; (k) autoritatea competentă responsabilă de cauza penală. În cazul în care concordanța confirmată se referă la date neidentificate sau urme, setul de date de bază menționat la al doilea paragraf conține următoarele date, în măsura în care sunt disponibile: (a) data la care și locul unde au fost obținute datele biometrice; (b) infracțiunea pentru care au fost obținute datele biometrice; (c) numărul cauzei penale; (d) autoritatea competentă responsabilă de cauza penală. Returnarea datelor de bază de către statul membru solicitat face obiectul unei decizii luate de un factor uman.			
(7) Utilizarea de către Europol a informațiilor obținute în urma unei interogări efectuate în conformitate cu prezentul articol și a schimbului unui set de date de bază în conformitate cu alineatul (6) este condiționată de acordul statului membru în a cărui bază de date s-a obținut concordanța. Dacă statul membru permite utilizarea informațiilor respective, gestionarea acestora de către Europol intră sub incidența Regulamentului (UE) 2016/794.		Prevedere UE neaplicabilă	Prevederea nu este aplicabilă pentru transpunere în legislația Republicii Moldova, întrucât reglementează drepturi și competențe instituționale ale Europol, agenție a Uniunii Europene, care decurg exclusiv din statutul de stat membru al UE.
Articolul 50. Scopul prelucrării datelor (1) Prelucrarea datelor cu caracter personal primite de către un stat membru sau		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i>

de către Europol este permisă numai în scopurile pentru care datele au fost transmise de statul membru care a furnizat datele în conformitate cu prezentul regulament. Prelucrarea în alte scopuri este permisă numai cu autorizarea prealabilă a statului membru care a furnizat datele.			Articolul 46. Protecția și scopul prelucrărilor datelor cu caracter personal (2) Schimbul de date cu statele membre ale Uniunii Europene se realizează în condițiile stabilite prin actele normative de cooperare aplicabile și după asigurarea funcționalității mecanismelor de protecție a datelor prevăzute de prezenta lege. (3) Prelucrarea datelor în alte scopuri decât cele prevăzute de prezenta lege se admite numai cu autorizarea prealabilă a statului participant sau a Europol (după caz), precum și în condițiile expres prevăzute de legislația națională.
(2) Prelucrarea datelor furnizate de către un stat membru sau Europol în temeiul articolului 6, 11, 16, 20 sau 26 este permisă doar dacă este necesară în scopul: (a) de a stabili dacă între profilurile ADN, datele dactiloscopice, datele privind înmatricularea vehiculelor, imaginile faciale sau evidențele poliției comparate există concordanțe; (b) de a face schimb de un set de date de bază în conformitate cu articolul 47; (c) de a pregăti și a depune o cerere formulată de organele de poliție sau judiciare în vederea acordării de asistență juridică, dacă s-a obținut o concordanță între date; (d) de a păstra înregistrări astfel cum se prevede la articolele 18, 40 și 45.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 46. Protecția și scopul prelucrărilor datelor cu caracter personal (4) Prelucrarea datelor furnizate de către statele membre ale Uniunii Europene sau de către Europol autorităților competente este permisă exclusiv dacă este necesară pentru: a) stabilirea existenței unei concordanțe între profilurile ADN, datele dactiloscopice, datele privind înmatricularea vehiculelor, imaginile faciale sau evidențele poliției comparate;

			b) efectuarea schimbului setului de date de bază în urma unei concordanțe confirmate; c) pregătirea și depunerea unei cereri de către organele de drept sau judiciare în vederea acordării de asistență juridică, în cazul obținerii unei concordanțe; d) păstrarea înregistrărilor (log-urilor) necesare pentru monitorizarea legalității și securității datelor.
(3) Datele primite de un stat membru sau de Europol se șterg imediat după răspunsurile automatizate la căutări, cu excepția cazului în care este necesară o prelucrare suplimentară în scopurile menționate la alineatul (2) sau o asemenea prelucrare este autorizată în conformitate cu alineatul (1).		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 46. Protecția și scopul prelucrărilor datelor cu caracter personal (5) Datele primite de către autoritățile competente de la Europol sau statele membre ale Uniunii Europene se șterg imediat după primirea răspunsurilor automatizate la căutări, cu excepția cazului în care este necesară o prelucrare ulterioară în scopurile prevăzute la alin. (4) ori în cazul în care prelucrarea este autorizată conform alin. (1).
(4) Înainte de a-și conecta bazele de date naționale la router sau la EPRIS, statele membre efectuează o evaluare a impactului asupra protecției datelor, astfel cum se menționează la articolul 27 din Directiva (UE) 2016/680, și, după caz, consultă autoritatea de supraveghere astfel cum se prevede la		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 46. Protecția și scopul prelucrărilor datelor cu caracter personal

articolul 28 din directiva respectivă. Autoritatea de supraveghere poate face uz de oricare dintre competențele care îi revin în temeiul articolului 47 din directiva respectivă, în conformitate cu articolul 28 alineatul (5) din directiva respectivă.			(6) Înainte de conectarea bazelor de date naționale la Router, EPRIS sau alte sisteme informaționale, autoritățile competente ale Republicii Moldova efectuează o evaluare a impactului operațiunilor de prelucrare asupra protecției datelor și consultă Centrul Național pentru Protecția Datelor cu Caracter Personal, conform cadrului normativ național. Evaluarea cuprinde cel puțin o descriere generală a operațiunilor de prelucrare preconizate, o evaluare a riscurilor la adresa drepturilor și libertăților persoanelor, măsurile preconizate în vederea gestionării riscurilor, garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal. (7) Agenția de Guvernare Electronică exercită atribuțiile de control pentru a asigura conformitatea procesului de interconectare cu standardele de securitate.
Articolul 51. Exactitatea, relevanța și păstrarea datelor (1) Statele membre și Europol asigură exactitatea și relevanța datelor cu caracter personal care sunt prelucrate în temeiul prezentului regulament. În cazul în care un stat membru sau Europol constată că au fost furnizate date care sunt incorecte sau nu mai	<i>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</i> Anexa nr.1 Punctul 40. În cadrul schimburilor de informații reglementate de prezentul capitol,	Compatibil	

sunt actuale sau date care nu ar fi trebuit furnizate, acesta notifică acest lucru statului membru care a primit datele sau Europol fără întârzieri nejustificate. Toate statele membre în cauză sau Europol corectează sau șterg datele în consecință, fără întârzieri nejustificate. În cazul în care statul membru care a primit datele sau Europol are motive să creadă că datele furnizate sunt incorecte sau ar trebui șterse, acesta informează statul membru care a furnizat datele fără întârzieri nejustificate.	PUC asigură respectarea următoarelor standarde de calitate și protecție a datelor: 40.1. datele cu caracter personal furnizate sunt exacte, complete și actualizate; Punctul 96. În cazul constatării furnizării unor date incorecte, neactuale sau care nu ar fi trebuit furnizate, PUC notifică imediat autoritatea destinatară, asigurând corectarea sau ștergerea acestora fără întârzieri nejustificate.		
(2) Statele membre și Europol instituie măsuri adecvate pentru actualizarea datelor relevante în sensul prezentului regulament.	<i>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</i> Anexa nr.2 Punctul 8. PNC își desfășoară activitatea în baza următoarelor principii specifice prelucrării datelor biometrice și alfanumerice: 8.1. <i>principiul exactității și actualizării</i> — asigurarea caracterului veridic al datelor din registrele naționale și rectificarea sau ștergerea imediată a informațiilor incorecte;	Compatibil	
(3) În cazul în care o persoană vizată a contestat exactitatea datelor aflate în posesia unui stat membru sau a Europol, dacă exactitatea nu poate fi stabilită în mod fiabil de către statul membru în cauză sau Europol și dacă persoana vizată solicită acest lucru, datele în cauză sunt marcate cu un marcaj. În cazul în care există un astfel de marcaj, statele membre sau Europol îl pot elimina numai cu permisiunea persoanei vizate sau pe baza unei decizii a instanței competente sau a autorității	<i>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</i> Anexa nr.1 Punctul 105. La cererea unei persoane vizate, PUC, în strânsă colaborare cu autoritatea competentă deținătoare a datelor (PNC), furnizează informații privind categoriile de date prelucrate, originea	Compatibil	

de supraveghere sau a Autorității Europene pentru Protecția Datelor, după caz.	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. Punctul 106. 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.		
(4) Datele cu caracter personal care nu ar fi trebuit să fie furnizate sau primite se șterg. Datele care sunt legal furnizate și primite se șterg: (a) dacă nu sunt sau nu mai sunt necesare pentru scopul pentru care au fost furnizate; (b) după expirarea termenului maxim de păstrare a datelor prevăzut de dreptul intern al statului membru care a furnizat datele, dacă statul membru respectiv a informat statul membru care a primit datele sau Europol cu privire la acest termen maxim la momentul furnizării datelor; sau (c) după expirarea perioadei maxime de păstrare a datelor prevăzute în Regulamentul (UE) 2016/794.	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 Anexa nr.1 Punctul 101. Datele cu caracter personal primite sau furnizate legal de către PUC se șterg din evidențele sale operative: 101.1. imediat ce se constată că nu mai sunt necesare pentru scopul pentru care au fost schimbate; 101.2. la primirea unei notificări de la Punctul Național de Contact (PNC) privind expirarea termenului de păstrare în registrul sursă, conform legislației naționale; 101.3. după expirarea perioadei maxime de păstrare prevăzute în Regulamentul (UE) 2016/794 privind Europol, pentru datele schimbate prin acest canal;	Compatibil	
În cazul în care există motive să se creadă că ștergerea datelor ar aduce atingere	Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic	Compatibil	

intereselor persoanei vizate, se restricționează prelucrarea datelor, în loc ca acestea să fie șterse. În cazul în care s-a restricționat prelucrarea datelor, acestea se prelucrează doar în scopul care a împiedicat ștergerea lor.	de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații Anexa nr.1 Punctul 100. 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. Anexa nr.2 Punctul 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.		
Articolul 52. Persoana împuternicită de operatorul de date (1) eu-LISA este persoana împuternicită de operator în înțelesul articolului 3 punctul 12 din Regulamentul (UE) 2018/1725 pentru prelucrarea datelor cu caracter personal prin intermediul routerului.		Normă UE neaplicabilă	Dispoziție care stabilește statutul juridic al agențiilor Uniunii Europene (eu-LISA și Europol) în calitate de persoane împuternicite de operator în temeiul Regulamentului (UE) 2018/1725. Reglementează exclusiv arhitectura instituțională și regimul de protecție a datelor aplicabil instituțiilor UE. Nu

			crează obligații pentru autoritățile naționale ale Republicii Moldova.
(2) Europol este persoana împuternicită de operator în înțelesul articolului 3 punctul 12 din Regulamentul (UE) 2018/1725 pentru prelucrarea datelor cu caracter personal prin intermediul EPRIS.		Normă UE neaplicabilă	Dispoziție care stabilește statutul juridic al agențiilor Uniunii Europene (eu-LISA și Europol) în calitate de persoane împuternicite de operator în temeiul Regulamentului (UE) 2018/1725. Reglementează exclusiv arhitectura instituțională și regimul de protecție a datelor aplicabil instituțiilor UE. Nu creează obligații pentru autoritățile naționale ale Republicii Moldova.
Articolul 53. Securitatea prelucrărilor de date (1) Autoritățile competente ale statelor membre, eu-LISA și Europol asigură securitatea prelucrării datelor cu caracter personal în temeiul prezentului regulament. Autoritățile competente ale statelor membre, eu-LISA și Europol cooperează în ceea ce privește atribuțiile legate de securitate.	<i>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</i> Anexa nr.1 Punctul 89. 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. PNC coordonează și monitorizează la nivel operațional integritatea acestui schimb, cooperând cu eu-LISA și Europol.	Prevedere UE netranspusă	Prevederile urmează să se regăsească în proiectul HG pentru aprobarea Instrucțiunii privind schimbul automatizat de date pentru cooperarea polițienească (Prüm II) și stabilirea punctelor naționale de contact.
(2) Fără a aduce atingere articolului 33 din Regulamentul (UE) 2018/1725 și articolului 32 din Regulamentul (UE) 2016/794, eu-LISA și Europol iau măsurile necesare pentru a asigura securitatea routerului și, respectiv, a		Prevedere UE neaplicabile	Prevederile sunt neaplicabile deoarece reglementează sarcini de securitate cibernetică și administrare tehnică în competența exclusivă a agențiilor Uniunii Europene (eu-LISA și

EPRIS, precum și a infrastructurii de comunicații aferente acestora.			Europol), asupra cărora Republica Moldova nu are jurisdicție legislativă.
(3) eu-LISA adoptă măsurile necesare cu privire la router, iar Europol adoptă măsurile necesare cu privire la EPRIS, în următoarele scopuri: (a) de a proteja fizic datele, inclusiv prin elaborarea de planuri de urgență pentru protejarea infrastructurii critice; (b) de a interzice accesul persoanelor neautorizate la echipamentele și instalațiile de prelucrare a datelor; (c) de a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a suporturilor de date; (d) de a împiedica introducerea neautorizată de date, precum și orice inspectare, modificare sau ștergere neautorizată a datelor cu caracter personal înregistrate; (e) de a împiedica prelucrarea neautorizată de date, precum și orice copiere, modificare sau ștergere neautorizată a datelor; (f) de a împiedica utilizarea sistemelor de prelucrare automată a datelor de către persoane neautorizate prin utilizarea echipamentelor de comunicare de date; (g) de a se asigura, prin utilizarea exclusivă a unor nume de utilizator individuale și a unor coduri de acces confidențiale, că persoanele autorizate să acceseze routerul sau EPRIS, după caz, au acces numai la datele care fac obiectul autorizației lor de acces;		Prevedere UE neaplicabilă	Prevederea stabilește obligații de securitate fizică și tehnică pentru agențiile Uniunii Europene (eu-LISA și Europol) în raport cu infrastructura centrală a sistemului Prüm II.

(h) de a asigura posibilitatea de a verifica și de a stabili care sunt organismele cărora le pot fi furnizate datele cu caracter personal prin utilizarea echipamentelor de comunicare de date; (i) de a asigura posibilitatea de a verifica și de a stabili ce date au fost prelucrate în router sau EPRIS, după caz, și în ce moment, de către cine și în ce scop au fost prelucrate; (j) de a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transmiterii acestora către sau din router sau EPRIS, după caz, sau în timpul transportului suporturilor de date, în special prin intermediul unor tehnici de criptare corespunzătoare; (k) de a asigura că, în cazul unei întreruperi, sistemele instalate pot fi readuse la funcționarea normală; (l) de a asigura fiabilitatea prin garantarea faptului că este raportată în mod adecvat orice deficiență în funcționarea routerului sau a EPRIS, după caz; (m) de a monitoriza eficacitatea măsurilor de securitate prevăzute la prezentul alineat și de a lua măsurile organizatorice necesare referitoare la monitorizarea internă, astfel încât să se asigure respectarea dispozițiilor prezentului regulament și să se evalueze măsurile de securitate respective în contextul noilor evoluții tehnologice.			
Articolul 54. Incidente de securitate (1) Orice eveniment care are sau poate avea un impact asupra securității routerului sau a EPRIS și care poate cauza daune sau	<i>Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de</i>	Compatibil	

pierderi ale datelor stocate în router sau EPRIS se consideră a fi un incident de securitate, în special în cazul în care este posibil să se fi accesat datele în mod neautorizat sau în cazul în care disponibilitatea, integritatea și confidențialitatea datelor au fost sau este posibil să fi fost compromise.	<i>Contact în scopul schimbului de date și informații</i> Anexa nr.1 Punctul 5. Prezentei Regulament, i se aplică noțiunile din Legea nr. XXX/2026 privind cooperarea polițienească internațională, precum și noțiunile utilizate cu următoarele semnificații: <i>5.6.incident semnificativ de securitate cibernetică</i> – orice eveniment care are sau poate avea un impact major asupra funcționării infrastructurii Router-ului ori a sistemului EPRIS sau care periclitează disponibilitatea, integritatea și confidențialitatea datelor biometrice ori alfanumerice prelucrate, fiind de natură să cauzeze pierderi de date sau accesări neautorizate și să necesite notificarea partenerilor internaționali;		
(2) În cazul unui incident de securitate privind routerul, eu-LISA și statele membre vizate sau, după caz, Europol cooperează între ele pentru a asigura un răspuns rapid, eficace și corespunzător.	<i>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</i> Anexa nr.1 Punctul 89. 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.	Compatibil	

(3) În cazul unui incident de securitate privind EPRIS, statele membre vizate și Europol cooperează între ele pentru a asigura un răspuns rapid, eficient și corespunzător.	<i>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</i> Anexa nr.1 Punctul 89. 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.	Compatibil	
(4) Statele membre notifică fără întârzieri nejustificate orice incident de securitate autorităților lor competente. Fără a aduce atingere articolului 92 din Regulamentul (UE) 2018/1725, în cazul unui incident de securitate legat de infrastructura centrală a routerului, eu-LISA notifică Serviciul de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile Uniunii (CERT-UE) cu privire la amenințările cibernetice semnificative, la vulnerabilitățile semnificative și la incidentele semnificative, fără întârzieri nejustificate și, în orice caz, în termen de cel mult 24 de ore din momentul în care ia cunoștință de acestea. Detaliile tehnice operative și adecvate privind amenințările cibernetice, vulnerabilitățile și incidentele care permit detectarea proactivă, răspunsul la incidente sau măsurile de atenuare sunt	<i>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</i> Anexa nr.1 Punctul 92. 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.	Compatibil	

comunicate către CERT-UE fără întârzieri nejustificate. Fără a aduce atingere articolului 34 din Regulamentul (UE) 2016/794 și articolului 92 din Regulamentul (UE) 2018/1725, în cazul unui incident de securitate legat de infrastructura centrală a EPRIS, Europol notifică CERT-UE cu privire la amenințările cibernetice semnificative, la vulnerabilitățile semnificative și la incidentele semnificative, fără întârzieri nejustificate și, în orice caz, în termen de cel mult 24 de ore din momentul în care ia cunoștință de acestea. Detaliile tehnice operative și adecvate privind amenințările cibernetice, vulnerabilitățile și incidentele care permit detectarea proactivă, răspunsul la incidente sau măsurile de atenuare sunt comunicate către CERT-UE fără întârzieri nejustificate.			
(5) Informațiile privind un incident de securitate care are sau poate avea un impact asupra funcționării routerului sau asupra disponibilității, integrității și confidențialității datelor sunt puse fără întârziere la dispoziția statelor membre și a Europol de către statele membre și agențiile Uniunii și se raportează în conformitate cu planul de gestionare a incidentelor care urmează să fie furnizat de eu-LISA.	<i>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</i> Anexa nr.1 Punctul 91. În scopul protejării infrastructurii tehnice, autoritatea competentă sau PNC implementează următoarele măsuri de securitate în cadrul sistemelor proprii: 91.1. protecția fizică a echipamentelor și instalațiilor de prelucrare a datelor; 91.2. împiedicarea accesului neautorizat la suporturile de date și echipamentele de prelucrare;	Compatibil	

	91.3. utilizarea mecanismelor de autentificare securizată (nume de utilizator individuale și coduri de acces) pentru personalul autorizat; 91.4. aplicarea tehnicilor de criptare corespunzătoare pentru transportul datelor către infrastructurile centrale; 91.5. asigurarea planurilor de redresare în caz de dezastru pentru restabilirea funcționării sistemelor. Punctul 92. 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.		
(6) Informațiile privind un incident de securitate care are sau poate avea un impact asupra funcționării EPRIS sau asupra disponibilității, integrității și confidențialității datelor sunt puse fără întârziere la dispoziția statelor membre de către statele membre și agențiile Uniunii și se raportează în conformitate cu planul de gestionare a incidentelor care urmează să fie furnizat de Europol.	<i>Proiectul Hotărârii de Guvern cu privire la înstituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații</i> Anexa nr.1 Punctul 91. În scopul protejării infrastructurii tehnice, autoritatea competentă sau PNC implementează următoarele măsuri de securitate în cadrul sistemelor proprii: 91.1. protecția fizică a echipamentelor și instalațiilor de prelucrare a datelor; 91.2. împiedicarea accesului neautorizat la suporturile de date și echipamentele de prelucrare; 91.3. utilizarea mecanismelor de autentificare securizată (nume de utilizator	Compatibil	

	individuale și coduri de acces) pentru personalul autorizat; 91.4. aplicarea tehnicilor de criptare corespunzătoare pentru transportul datelor către infrastructurile centrale; 91.5. asigurarea planurilor de redresare în caz de dezastru pentru restabilirea funcționării sistemelor. Punctul 92. 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.		
Articolul 55. Automonitorizarea (1) Statele membre se asigură că fiecare autoritate care are dreptul de a utiliza cadrul Prüm II ia măsurile necesare pentru a monitoriza respectarea prezentului regulament și cooperează, dacă este cazul, cu autoritatea națională de supraveghere. Europol ia măsurile necesare pentru a monitoriza respectarea prezentului regulament și cooperează, dacă este necesar, cu Autoritatea Europeană pentru Protecția Datelor.		Parțial compatibilă	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 48. Automonitorizarea (1) Autoritatea competentă ia măsurile necesare pentru a respecta prezenta lege și cooperează cu Centrul Național pentru Protecția Datelor cu Caracter Personal. A doua parte din prevedere se referă la Europol și la cooperarea cu Autoritatea Europeană pentru Protecția Datelor nu se transpune, întrucât vizează regimul juridic al unei agenții a Uniunii Europene.

(2) Operatorii de date pun în aplicare măsurile necesare pentru a monitoriza efectiv respectarea dispozițiilor prezentului regulament pe parcursul prelucrării datelor, inclusiv prin verificarea frecvență a înregistrărilor menționate la articolele 18, 40 și 45. Aceștia cooperează, dacă este necesar și după caz, cu autoritățile de supraveghere sau cu Autoritatea Europeană pentru Protecția Datelor.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 48. Automonitorizarea (2) Operatorii de date implementează măsuri tehnice și organizatorice pentru a monitoriza respectarea prezentei legi, inclusiv prin verificarea anuală a înregistrărilor (log-urilor), activităților de prelucrare, conform cerințelor de audit stabilite de legislația națională și cooperează cu Centrul Național pentru Protecția Datelor cu Caracter Personal pentru a asigura transparența prelucrărilor.
Articolul 56. Sancțiuni Statele membre se asigură că orice utilizare abuzivă a datelor și orice prelucrare sau schimb de date care încalcă prezentul regulament sunt sancționate în conformitate cu dreptul intern. Sancțiunile prevăzute trebuie să fie efective, proporționale și cu efect de descurajare.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 49. Răspunderea (1) Persoanele vinovate pentru utilizarea abuzivă a datelor, prelucrarea sau schimbul de informații contrar prezentei legi, poartă răspunde în conformitate cu legislația privind protecția datelor cu caracter personal.
Articolul 57. Răspunderea Dacă orice nerespectare de către un stat membru sau, la efectuarea de interogări în conformitate cu articolul 49, de către Europol a obligațiilor care îi revin în temeiul prezentului regulament provoacă prejudicii routerului sau EPRIS, răspunderea aparține		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 49. Răspunderea (2) În cazul în care autoritatea competentă de aplicare a legii nu își îndeplinește obligațiile stabilite

statului membru respectiv sau Europol, cu excepția cazului în care eu-LISA, Europol sau un alt stat membru căruia îi revin obligații în temeiul prezentului regulament nu a luat măsuri rezonabile pentru a preveni producerea prejudiciului sau pentru a reduce la minimum impactul acestuia.			de prezenta lege și prin aceasta cauzează un prejudiciu Routerului, EPRIS sau altor sisteme informaționale, aceasta poartă răspundere civilă, în condițiile legii. (3) Autoritatea competentă de aplicare a legii este exonerată, total sau parțial, de răspunderea prevăzută la alin. (2) dacă dovedește că prejudiciul a fost cauzat de acțiunea sau inacțiunea eu-LISA, Europol ori a unui alt stat membru al Uniunii Europene, constând în neadoptarea măsurilor rezonabile pentru prevenirea producerii prejudiciului sau pentru limitarea consecințelor acestuia.
Articolul 58. Auditurile efectuate de Autoritatea Europeană pentru Protecția Datelor (1) Autoritatea Europeană pentru Protecția Datelor garantează că cel puțin o dată la patru ani se realizează un audit al operațiunilor de prelucrare a datelor cu caracter personal desfășurate de eu-LISA și de Europol, în sensul prezentului regulament, în conformitate cu standardele internaționale de audit relevante. Un raport al acestui audit se trimite Parlamentului European, Consiliului, Comisiei, statelor membre și agenției în cauză a Uniunii. eu-LISA și Europol au posibilitatea de a formula observații înainte de adoptarea rapoartelor.		Prevedere UE neaplicabilă	Prevederea reglementează competențele Autorității Europene pentru Protecția Datelor în raport cu instituțiile, organele și agențiile Uniunii Europene și cu infrastructura centrală a sistemului Prüm II.
(2) eu-LISA și Europol pun la dispoziția Autorității Europene pentru Protecția Datelor		Prevedere UE neaplicabilă	Prevederea reglementează competențele Autorității Europene

informațiile solicitate de aceasta și oferă Autorității Europene pentru Protecția Datelor acces la toate documentele solicitate de aceasta și la înregistrările lor menționate la articolele 40 și 45, precum și la toate sediile proprii, în orice moment. Prezentul alineat nu aduce atingere competențelor Autorității Europene pentru Protecția Datelor în temeiul articolului 58 din Regulamentul (UE) 2018/1725 și, în ceea ce privește Europol, în temeiul articolului 43 alineatul (3) din Regulamentul (UE) 2016/794.			pentru Protecția Datelor în raport cu instituțiile, organele și agențiile Uniunii Europene și cu infrastructura centrală a sistemului Prüm II.
Articolul 59. Cooperarea dintre autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor (1) Autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor, fiecare acționând în limitele competențelor sale, cooperează activ în cadrul responsabilităților lor pentru a asigura o supraveghere coordonată a aplicării prezentului regulament, în special dacă Autoritatea Europeană pentru Protecția Datelor sau o autoritate de supraveghere identifică discrepanțe majore între practicile statelor membre sau transferuri potențial ilegale efectuate prin canalele de comunicare ale cadrului Prüm II.	<i>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</i> Anexa nr.1 Punctul 104. Centrul Național pentru Protecția Datelor cu Caracter Personal (în continuare – CNPDPCP) exercită controlul asupra prelucrărilor efectuate de PUC și PNC, cooperând activ cu Autoritatea Europeană pentru Protecția Datelor (AEPD) în cadrul responsabilităților lor de supraveghere a Router-ului și a sistemului EPRIS.	Compatibil	
(2) În cazurile menționate la alineatul (1) de la prezentul articol, se asigură o supraveghere coordonată în conformitate cu articolul 62 din Regulamentul (UE) 2018/1725.	<i>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</i> Anexa nr.1 Punctul 104. Centrul Național pentru Protecția Datelor cu Caracter Personal (în	Compatibil	

	continuare – CNPDCP) exercită controlul asupra prelucrărilor efectuate de PUC și PNC, cooperând activ cu Autoritatea Europeană pentru Protecția Datelor (AEPD) în cadrul responsabilităților lor de supraveghere a Router-ului și a sistemului EPRIS.		
(3) La doi ani de la intrarea în funcțiune a routerului și a EPRIS și, ulterior, din doi în doi ani, Comitetul european pentru protecția datelor transmite Parlamentului European, Consiliului, Comisiei, eu-LISA și Europol un raport privind activitățile sale în temeiul prezentului articol. Raportul respectiv include un capitol despre fiecare stat membru, elaborat de autoritatea de supraveghere a statului membru respectiv.		Prevedere UE neaplicabilă	Prevederea reglementează obligațiile de raportare ale Comitetului european pentru protecția datelor către instituțiile UE.
Articolul 60. Transferul de date cu caracter personal către țări terțe și organizații internaționale Un stat membru transferă datele cu caracter personal pe care le-a obținut în temeiul prezentului regulament către o țară terță sau o organizație internațională numai în conformitate cu capitolul V din Directiva (UE) 2016/680 și cu condiția ca statul membru solicitat să fi acordat autorizația înainte de transfer.		Compatibilă	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 50. Transferul de date cu caracter personal către țări terțe și organizații internaționale (1) Autoritatea competentă poate transfera prin intermediul punctului unic de contact date cu caracter personal obținute în temeiul prezentei legi către un stat terț sau o organizație internațională, numai în condițiile prevăzute de legislația națională privind protecția datelor cu caracter personal și de actele normative aplicabile cooperării polițienesci internaționale, cu autorizarea prealabilă a statului participant care a furnizat datele

			respective, cu condiția existenței unei decizii sau a unor garanții care asigură un nivel de protecție echivalent cu standardele europene aplicabile prelucrărilor efectuate de autorități competente.
Europol transferă datele cu caracter personal pe care le-a obținut în temeiul prezentului regulament către o țară terță sau o organizație internațională numai dacă au fost îndeplinite condițiile prevăzute la articolul 25 din Regulamentul (UE) 2016/794 și cu condiția ca statul membru solicitat să fi acordat autorizația înainte de transfer.		Compatibilă	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 50. Transferul de date cu caracter personal către țări terțe și organizații internaționale (2) În cazul în care datele furnizate de autoritățile competente ale Republicii Moldova sunt prelucrate ulterior de Europol, autorizarea pentru transferul acestora către un stat terț sau o organizație internațională se acordă de autoritatea competentă națională.
Articolul 61. Relația cu alte acte juridice privind protecția datelor Orice prelucrare a datelor cu caracter personal în sensul prezentului regulament se efectuează în conformitate cu prezentul capitol și cu Directiva (UE) 2016/680 sau Regulamentul (UE) 2018/1725, Regulamentul (UE) 2016/794 sau Regulamentul (UE) 2016/679, după caz.		Compatibilă	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 50. Transferul de date cu caracter personal către țări terțe și organizații internaționale (3) Prelucrarea datelor cu caracter personal în cadrul mecanismului prevăzut de prezenta lege se efectuează cu respectarea cadrului normativ privind protecția datelor cu caracter personal, în măsura în care prezenta lege nu prevede dispoziții speciale.

Articolul 62. Responsabilitatea pentru diligența necesară Statele membre și Europol exercită diligența necesară atunci când evaluează dacă schimbul automatizat de date se încadrează în obiectivul cadrului Prüm II prevăzut la articolul 2 și dacă acesta respectă condițiile prevăzute la articolul respectiv, în special în ceea ce privește respectarea drepturilor fundamentale.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 51. Responsabilitatea și instruirea (1) Autoritatea competentă și Europol evaluează dacă schimbul automatizat de date se încadrează în obiectivele prezentei legi și dacă acesta respectă condițiile stabilite, în special în ceea ce privește garantarea și respectarea drepturilor fundamentale ale omului.
Articolul 63. Formarea Personalul autorizat al autorităților competente ale statelor membre, al autorităților de supraveghere și al Europol beneficiază, după caz, de resurse și formare adecvate, inclusiv în ceea ce privește protecția datelor și examinarea exactă a concordanțelor, pentru a îndeplini sarcinile prevăzute în prezentul regulament.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 51. Responsabilitatea și instruirea (2) Autoritățile competente asigură, după caz, personalului autorizat implicat în aplicarea prezentei legi, resursele necesare și formarea profesională pentru îndeplinirea atribuțiilor. (3) Formarea prevăzută la alin. (2) include, în mod obligatoriu, instruirea privind: a) protecția datelor cu caracter personal și securitatea informației în cadrul schimbului de date realizat în temeiul prezentei legi; b) verificarea și confirmarea exactă a concordanțelor/rezultatelor obținute în urma căutărilor și

			comparațiilor efectuate, inclusiv prin proceduri de examinare manuală atunci când este cazul. (4) Autoritățile competente și după caz, autoritatea de supraveghere din domeniul protecției datelor cu caracter personal asigură că personalul autorizat are acces la resurse tehnice și organizatorice, proporționale cu volumul și natura operațiunilor realizate în temeiul prezentei legi.
Articolul 64. Responsabilitățile statelor membre (1) Fiecare stat membru este responsabil pentru: (a) conectarea la infrastructura routerului; (b) integrarea sistemelor și infrastructurii sale naționale existente cu routerul; (c) organizarea, gestionarea, exploatarea și întreținerea infrastructurii naționale existente și conectarea acesteia la router; (d) conectarea la infrastructura EPRIS; (e) integrarea sistemelor și infrastructurii sale naționale existente cu EPRIS; (f) organizarea, gestionarea, exploatarea și întreținerea infrastructurii sale naționale existente și conectarea acesteia la EPRIS; (g) gestionarea accesului și modalitățile de accesare a routerului de către personalul autorizat în mod corespunzător al autorităților sale competente, în conformitate cu prezentul regulament, precum și crearea și actualizarea periodică a unei liste a membrilor personalului respectiv și a profilurilor acestora;		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 51. Responsabilitatea și instruirea (5) Autoritățile competente desemnate potrivit prezentei legi, asigură: a) conectarea la infrastructura Router-ului, sistemului EPRIS sau altor sisteme informaționale, în condițiile tehnice stabilite pentru schimbul de date realizat în temeiul prezentei legi; b) integrarea sistemelor și infrastructurii naționale existente cu Router-ul, EUCARIS, sistemul EPRIS sau alte sisteme informaționale; c) organizarea, administrarea, operarea și întreținerea infrastructurii naționale utilizate pentru schimbul de date și

(h) gestionarea accesului și modalitățile de accesare a EPRIS de către personalul autorizat în mod corespunzător al autorităților sale competente, în conformitate cu prezentul regulament, precum și crearea și actualizarea periodică a unei liste a membrilor personalului respectiv și a profilurilor acestora; (i) gestionarea accesului și modalitățile de accesare a Eucaris de către personalul autorizat în mod corespunzător al autorităților sale competente, în conformitate cu prezentul regulament, precum și crearea și actualizarea periodică a unei liste a membrilor personalului respectiv și a profilurilor acestora; (j) confirmarea manuală de către membri ai personalului calificat a unei concordanțe, astfel cum se menționează la articolul 6 alineatele (6) și (7), articolul 11 alineatul (2) și articolul 20 alineatul (2); (k) asigurarea disponibilității datelor necesare pentru schimbul de date în conformitate cu articolele 5, 10, 16, 19 și 25; (l) schimbul de informații în conformitate cu articolele 6, 11, 16, 20 și 26; (m) corectarea, actualizarea sau ștergerea oricăror date primite de la un stat membru solicitat în termen de 48 de ore de la notificarea statului membru solicitat cu privire la faptul că datele transmise au fost incorecte, nu mai sunt actualizate sau au fost transmise ilegal; (n) conformitatea cu cerințele de calitate a datelor stabilite în prezentul regulament.		conectarea acestora la Router, EUCARIS, sistemul EPRIS sau alte sisteme informaționale; d) gestionarea accesului și a modalităților de accesare a Router-ului, sistemului EPRIS sau altor sisteme informaționale de către personalul autorizat al autorităților competente, inclusiv stabilirea drepturilor de acces, autentificarea și trasabilitatea accesărilor, precum și întocmirea și actualizarea periodică a listei persoanelor autorizate și a profilurilor acestora; e) confirmarea manuală a concordanțelor/rezultatelor obținute în urma căutărilor automatizate, de către membri ai personalului calificat, în cazurile și potrivit procedurilor prevăzute de prezenta lege; f) asigurarea disponibilității și accesibilității datelor necesare pentru schimbul de date realizat în temeiul prezentei legi, în limitele competențelor legale ale autorităților competente și cu respectarea cerințelor de protecție a datelor; g) schimbul ulterior de informații, verificările suplimentare și cooperarea polițienească operațională, prin intermediul punctului unic de contact în cazurile și potrivit

			procedurilor prevăzute de prezenta lege; h) corectarea, actualizarea sau ștergerea, după caz, a datelor primite de la o autoritate parteneră, în termen de cel mult 48 de ore de la primirea notificării că datele transmise au fost inexacte, neactuale ori au fost transmise cu încălcarea legii, cu informarea fără întârziere a autorității care a furnizat datele; i) respectarea cerințelor de calitate a datelor aplicabile schimbului de date realizat în temeiul prezentei legi, inclusiv a regulilor privind acuratețea, actualitatea, completitudinea și relevanța acestora.
Articolul 65. Responsabilitățile Europol (1) Europol este responsabil pentru gestionarea accesului și modalitățile de accesare a routerului, a EPRIS și a Eucaris de către personalul său autorizat în mod corespunzător, în conformitate cu prezentul regulament.		Prevedere UE neaplicabilă	Reglementează gestiunea tehnică a sistemului EPRIS de către Europol și adaptarea infrastructurii acesteia.
(2) Europol este responsabil pentru prelucrarea interogărilor în datele Europol de către router. Europol își adaptează sistemele de informații în consecință.		Prevedere UE neaplicabilă	Reglementează gestiunea tehnică a sistemului EPRIS de către Europol și adaptarea infrastructurii acesteia.
(3) Europol este responsabil pentru orice adaptări tehnice ale infrastructurii Europol necesare pentru stabilirea conectării la router și la Eucaris.		Prevedere UE neaplicabilă	Reglementează gestiunea tehnică a sistemului EPRIS de către Europol și adaptarea infrastructurii acesteia.
(4) Fără a aduce atingere căutărilor efectuate de Europol în temeiul articolului 49,		Prevedere UE neaplicabilă	Reglementează gestiunea tehnică a sistemului EPRIS de către

Europol nu are acces la niciuna dintre datele cu caracter personal prelucrate prin intermediul EPRIS.			Europol și adaptarea infrastructurii acesteia.
(5) Europol este responsabil pentru dezvoltarea EPRIS în cooperare cu statele membre. EPRIS oferă funcționalitățile prevăzute la articolele 42-46. Europol este responsabil pentru gestionarea tehnică a EPRIS. Gestionarea tehnică a EPRIS constă în toate sarcinile și soluțiile tehnice necesare pentru a menține funcționarea infrastructurii centrale a EPRIS și furnizarea neîntreruptă de servicii statelor membre, 24 de ore pe zi, 7 zile pe săptămână, în conformitate cu prezentul regulament. Gestionarea tehnică include lucrările de întreținere și dezvoltările tehnice necesare pentru a se asigura funcțiile EPRIS la un nivel satisfăcător de calitate tehnică, în special în ceea ce privește timpul de răspuns pentru transmiterea de solicitări către bazele de date naționale în conformitate cu specificațiile tehnice.		Prevedere UE neaplicabilă	Reglementează gestiunea tehnică a sistemului EPRIS de către Europol și adaptarea infrastructurii acesteia.
(6) Europol asigură formarea pentru utilizarea tehnică a EPRIS.		Prevedere UE neaplicabilă	Reglementează gestiunea tehnică a sistemului EPRIS de către Europol și adaptarea infrastructurii acesteia.
(7) Europol este responsabil pentru procedurile prevăzute la articolele 48 și 49.		Prevedere UE neaplicabilă	Reglementează gestiunea tehnică a sistemului EPRIS de către Europol și adaptarea infrastructurii acesteia.
Articolul 66. Responsabilitățile eu-LISA în etapa de concepere și dezvoltare a routerului		Prevedere UE neaplicabilă	Stabilesc obligațiile eu-Lisa privind dezvoltarea și gestionarea tehnică a Routerului central, fiind norme interne ale UE pentru agenția sa.

(1) eu-LISA se asigură că infrastructura centrală a routerului este exploatată în conformitate cu prezentul regulament.			
(2) Routerul este găzduit de eu-LISA în amplasamentele sale tehnice și asigură funcționalitățile prevăzute în prezentul regulament, în conformitate cu condițiile de securitate, disponibilitate, calitate și performanță menționate la articolul 67 alineatul (1).		Prevedere UE neaplicabilă	Stabilesc obligațiile eu-Lisa privind dezvoltarea și gestionarea tehnică a Routerului central, fiind norme interne ale UE pentru agenția sa.
(3) Agenția eu-LISA este responsabilă pentru dezvoltarea routerului și pentru orice adaptări tehnice necesare pentru funcționarea routerului.		Prevedere UE neaplicabilă	Stabilesc obligațiile eu-Lisa privind dezvoltarea și gestionarea tehnică a Routerului central, fiind norme interne ale UE pentru agenția sa.
(4) eu-LISA nu are acces la niciuna dintre datele cu caracter personal prelucrate prin router.		Prevedere UE neaplicabilă	Stabilesc obligațiile eu-Lisa privind dezvoltarea și gestionarea tehnică a Routerului central, fiind norme interne ale UE pentru agenția sa.
(5) eu-LISA definește modul în care este concepută arhitectura fizică a routerului, inclusiv a infrastructurii sale de comunicații securizată, precum și specificațiile tehnice și evoluția acestora în ceea ce privește infrastructura centrală și infrastructura de comunicații securizată. Consiliul de administrație al eu-LISA aprobă modul de concepere, sub rezerva unui aviz favorabil din partea Comisiei. De asemenea, eu-LISA pune în aplicare orice adaptare necesară a componentelor de interoperabilitate care rezultă din instituirea routerului, astfel cum se prevede în prezentul regulament.		Prevedere UE neaplicabilă	Stabilesc obligațiile eu-Lisa privind dezvoltarea și gestionarea tehnică a Routerului central, fiind norme interne ale UE pentru agenția sa.
(6) eu-LISA dezvoltă și implementează routerul cât mai curând posibil după adoptarea		Prevedere UE neaplicabilă	Stabilesc obligațiile eu-Lisa privind dezvoltarea și gestionarea

de către Comisie a măsurilor prevăzute la articolul 37 alineatul (6). Dezvoltarea respectivă constă în elaborarea și implementarea specificațiilor tehnice, efectuarea de teste și gestionarea și coordonarea generală a proiectului.			tehnică a Routerului central, fiind norme interne ale UE pentru agenția sa.
(7) În cursul etapei de concepere și dezvoltare, Consiliul de administrație al programului menționat la articolul 54 din Regulamentul (UE) 2019/817 și la articolul 54 din Regulamentul (UE) 2019/818 se reunește periodic. Acesta asigură gestionarea adecvată a etapei de concepere și dezvoltare a routerului. Consiliul de administrație al programului prezintă lunar Consiliului de administrație al eu-LISA rapoarte scrise privind evoluția proiectului. Consiliul de administrație al programului nu are competențe decizionale și nu dispune de un mandat pentru a-i reprezenta pe membrii Consiliului de administrație al eu-LISA. Grupul consultativ pentru interoperabilitate menționat la articolul 78 se reunește cu regularitate până la începerea funcționării routerului. După fiecare reuniune, acesta prezintă un raport Consiliului de administrație al programului. Grupul consultativ furnizează expertiza tehnică necesară în sprijinul atribuțiilor care revin Consiliului de administrație al programului și monitorizează stadiul de pregătire al statelor membre.		Prevedere UE neaplicabilă	Stabilesc obligațiile eu-Lisa privind dezvoltarea și gestionarea tehnică a Routerului central, fiind norme interne ale UE pentru agenția sa.
Articolul 67. Responsabilitățile eu-LISA după începerea funcționării routerului		Prevedere UE neaplicabilă	Prevederea stabilește responsabilitățile agenției Uniunii Europene eu-LISA în ceea ce

(1) După punerea în funcțiune a routerului, eu-LISA este responsabilă pentru gestionarea tehnică a infrastructurii centrale a routerului, inclusiv pentru întreținerea acestuia și pentru dezvoltările tehnologice. În cooperare cu statele membre, aceasta se asigură că se utilizează cea mai bună tehnologie disponibilă, sub rezerva unei analize cost-beneficiu. eu-LISA este, de asemenea, responsabilă pentru gestionarea tehnică a infrastructurii de comunicații necesare. Gestionarea tehnică a routerului cuprinde toate sarcinile și soluțiile tehnice necesare pentru a menține funcționarea routerului și furnizarea neîntreruptă de servicii statelor membre și Europol 24 de ore pe zi, 7 zile pe săptămână, în conformitate cu prezentul regulament. Gestionarea tehnică include lucrările de întreținere și dezvoltările tehnice necesare pentru a se asigura funcționarea routerului la un nivel satisfăcător de calitate tehnică, în special în ceea ce privește disponibilitatea și timpul de răspuns pentru transmiterea de solicitări către bazele de date naționale și către datele Europol în conformitate cu specificațiile tehnice. Routerul este dezvoltat și gestionat astfel încât să se asigure accesul rapid, eficient și controlat, o disponibilitate deplină și neîntreruptă, precum și un timp de răspuns în conformitate cu nevoile operaționale ale autorităților competente ale statelor membre și ale Europol.			privește funcționarea infrastructurii centrale a sistemului Prüm II (router).
(2) Fără a aduce atingere articolului 17 din Statutul funcționarilor Uniunii Europene prevăzut în Regulamentul (CEE, Euratom,		Prevedere UE neaplicabilă	Prevederea stabilește responsabilitățile agenției Uniunii Europene eu-LISA în ceea ce

CECO) nr. 259/68 al Consiliului(18), eu-LISA aplică norme corespunzătoare privind secretul profesional sau alte responsabilități echivalente de confidențialitate membrilor personalului său care trebuie să lucreze cu date stocate în router. Această obligație se aplică și după ce persoanele respective au încetat să mai ocupe o anumită funcție sau după ce și-au încetat activitatea. eu-LISA nu are acces la niciuna dintre datele cu caracter personal prelucrate prin router.			privește funcționarea infrastructurii centrale a sistemului Prüm II (router).
(3) eu-LISA îndeplinește sarcini legate de asigurarea formării privind utilizarea tehnică a routerului.		Prevedere UE neaplicabilă	Prevederea stabilește responsabilitățile agenției Uniunii Europene eu-LISA în ceea ce privește funcționarea infrastructurii centrale a sistemului Prüm II (router).
Articolul 72. Raportare și statistici (1) Dacă este necesar, personalul autorizat în mod corespunzător din cadrul autorităților competente ale statelor membre, din cadrul Comisiei, al eu-LISA și al Europol are acces la următoarele date referitoare la router, exclusiv în scopul întocmirii de rapoarte și statistici: (a) numărul de interogări pentru fiecare stat membru și numărul de interogări pentru Europol pe categorie de date; (b) numărul de interogări în fiecare dintre bazele de date conectate; (c) numărul de concordante cu baza de date a fiecărui stat membru pentru fiecare categorie de date; (d) numărul de concordante cu datele Europol pentru fiecare categorie de date;	<i>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</i> Anexa nr.1 Punctul 111. În scopul evaluării eficienței cooperării polițienești internaționale, monitorizării legale și auditului securității, autoritățile competente/punctele naționale de contact, 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. Punctul 115. Pentru schimbul automatizat de date biometrice (profiluri ADN, date	Compatibil	

(e) numărul de concordanțe confirmate în cazul cărora au avut loc schimburi de date de bază; (f) numărul de concordanțe confirmate în cazul cărora nu au avut loc schimburi de date de bază; (g) numărul de interogări în registrul comun de date de identitate prin router; și (h) numărul de concordanțe pe tip după cum urmează: (i) date identificate (persoană) – date neidentificate (urme); (ii) date neidentificate (urme) – date identificate (persoană); (iii) date neidentificate (urme) – date neidentificate (urme); (iv) date identificate (persoană) – date identificate (persoană). Datele prevăzute la primul paragraf nu trebuie să permită identificarea persoanelor.	dactiloscopice și imagini faciale) prin intermediul Router-ului, PUC colectează următoarele date: 115.1. numărul de interogări lansate de Republica Moldova și numărul de interogări primite de la fiecare stat membru și de la Europol, pe categorii de date; 115.2. numărul de interogări efectuate în fiecare dintre bazele de date conectate la Router; 115.3. numărul de concordanțe (hits) identificate în bazele de date naționale și în cele ale partenerilor; 115.4. numărul de concordanțe confirmate manual care au generat schimbul setului de date de bază; 115.5. numărul de concordanțe confirmate în cazul cărora nu a avut loc schimbul de date de bază; 115.6. numărul de interogări lansate simultan în CIR prin intermediul Router-ului; 115.7. tipul concordanțelor identificate, clasificate astfel: 115.7.1. date identificate (persoană) – date neidentificate (urme); 115.7.2. date neidentificate (urme) – date identificate (persoană); 115.7.3. date neidentificate (urme) – date neidentificate (urme); 115.7.4. date identificate (persoană) – date identificate (persoană). Punctul 114. 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.		
(2) Personalul autorizat în mod corespunzător din cadrul autorităților competente ale statelor membre, din cadrul Comisiei și al Europol are acces la următoarele date referitoare la Eucaris, exclusiv în scopul întocmirii de rapoarte și statistici: (a) numărul de interogări pentru fiecare stat membru și numărul de interogări pentru Europol; (b) numărul de interogări în fiecare dintre bazele de date conectate; și (c) numărul de concordanțe cu baza de date a fiecărui stat membru. Datele prevăzute la primul paragraf nu trebuie să permită identificarea persoanelor.	<i>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</i> Anexa nr.1 Punctul 111. În scopul evaluării eficienței cooperării polițienești internaționale, monitorizării legale și auditului securității, autoritățile competente/punctele naționale de contact, 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. Punctul 115. Pentru schimbul automatizat de date biometrice (profiluri ADN, date dactiloscopice și imagini faciale) prin intermediul Router-ului, PUC colectează următoarele date: 115.1. numărul de interogări lansate de Republica Moldova și numărul de interogări primite de la fiecare stat membru și de la Europol, pe categorii de date; 115.2. numărul de interogări efectuate în fiecare dintre bazele de date conectate la Router; 115.3. numărul de concordanțe (hits) identificate în bazele de date naționale și în cele ale partenerilor;	Compatibil	

	115.4. numărul de concordanțe confirmate manual care au generat schimbul setului de date de bază; 115.5. numărul de concordanțe confirmate în cazul cărora nu a avut loc schimbul de date de bază; 115.6. numărul de interogări lansate simultan în CIR prin intermediul Router-ului; 115.7. tipul concordanțelor identificate, clasificate astfel: 115.7.1. date identificate (persoană) – date neidentificate (urme); 115.7.2. date neidentificate (urme) – date identificate (persoană); 115.7.3. date neidentificate (urme) – date neidentificate (urme); 115.7.4. date identificate (persoană) – date identificate (persoană). Punctul 114. 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.		
(3) Personalul autorizat în mod corespunzător din cadrul autorităților competente ale statelor membre, din cadrul Comisiei și al Europol are acces la următoarele date referitoare la EPRIS, exclusiv în scopul întocmirii de rapoarte și statistici:	<i>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</i> Anexa nr.1 Punctul 111. În scopul evaluării eficienței cooperării polițienești internaționale,	Compatibil	

(a) numărul de interogări pentru fiecare stat membru și numărul de interogări pentru Europol; (b) numărul de interogări în fiecare dintre registrele conectate; și (c) numărul de concordanțe cu baza de date a fiecărui stat membru. Datele prevăzute la primul paragraf nu trebuie să permită identificarea persoanelor.	monitorizării legale și auditului securității, autoritățile competente/punctele naționale de contact, 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. Punctul 115. Pentru schimbul automatizat de date biometrice (profiluri ADN, date dactiloscopice și imagini faciale) prin intermediul Router-ului, PUC colectează următoarele date: 115.1. numărul de interogări lansate de Republica Moldova și numărul de interogări primite de la fiecare stat membru și de la Europol, pe categorii de date; 115.2. numărul de interogări efectuate în fiecare dintre bazele de date conectate la Router; 115.3. numărul de concordanțe (hits) identificate în bazele de date naționale și în cele ale partenerilor; 115.4. numărul de concordanțe confirmate manual care au generat schimbul setului de date de bază; 115.5. numărul de concordanțe confirmate în cazul cărora nu a avut loc schimbul de date de bază; 115.6. numărul de interogări lansate simultan în CIR prin intermediul Router-ului; 115.7. tipul concordanțelor identificate, clasificate astfel: 115.7.1. date identificate (persoană) – date neidentificate (urme);		

	115.7.2. date neidentificate (urme) – date identificate (persoană); 115.7.3. date neidentificate (urme) – date neidentificate (urme); 115.7.4. date identificate (persoană) – date identificate (persoană). Punctul 114. 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.		
(4) eu-LISA stochează datele prevăzute la alineatul (1) de la prezentul articol în registrul central de raportare și statistici instituit prin articolul 39 din Regulamentul (UE) 2019/818. Europol stochează datele prevăzute la alineatul (3). Datele respective permit autorităților competente ale statelor membre, Comisiei, eu-LISA și Europol să obțină rapoarte și statistici adaptabile pentru a spori eficiența cooperării în materie de asigurare a respectării legii.		Prevedere UE neaplicabile	Prevederea stabilește atribuțiile agențiilor UE privind sisteme centrale și de stocare a datelor.
Articolul 73. Costuri (1) Costurile aferente instituirii și funcționării routerului și a EPRIS sunt suportate din bugetul general al Uniunii.		Prevedere UE neaplicabilă	Prevederea reglementează repartizarea costurilor în bugetul UE pentru instituirea și funcționarea routerului și a EPRIS.
(2) Costurile aferente integrării infrastructurii naționale existente și conexiunile acesteia cu routerul și EPRIS, precum și costurile suportate în legătură cu crearea bazelor de date naționale cu imagini		Prevedere UE neaplicabilă	Prevederea reglementează repartizarea costurilor în bugetul UE pentru integrarea infrastructurii naționale existente

faciale și a registrelor naționale ale evidențelor poliției pentru prevenirea, depistarea și investigarea infracțiunilor sunt suportate din bugetul general al Uniunii.			și conexiunile acestora cu routerul și EPRIS.
Sunt excluse următoarele costuri: (a) costurile aferente birourilor de gestionare a proiectelor din statele membre (reuniuni, misiuni, spații de lucru); (b) costurile aferente găzduirii sistemelor informatice naționale (spații, implementare, energie electrică, răcire); (c) costurile aferente exploatării sistemelor informatice naționale (operatori și contracte de asistență); (d) costurile aferente conceperii, dezvoltării, implementării, exploatării și întreținerii rețelelor naționale de comunicații.		Prevedere UE neaplicabile	Prevederea reglementează derogări de la unele costuri suportate din bugetul general al Uniunii.
(3) Fiecare stat membru suportă costurile care decurg din administrarea, utilizarea și întreținerea Eucaris. (4) Fiecare stat membru suportă costurile care decurg din administrarea, utilizarea și întreținerea conexiunilor sale cu routerul și EPRIS.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 52. Costuri (1) Autoritățile competente suportă costurile de administrare, utilizare și mentenanță a sistemelor de schimb automatizat de date EUCARIS, router și EPRIS, inclusiv conexiunile și infrastructura aferentă din bugetele aprobate. (2) În situații speciale, ce vizează operațiunile comune, misiunile de asistență în caz de dezastre sau detașarea de specialiști, autoritățile competente de aplicare a legii pot stabili de comun acord cu statele membre

			ale Uniunii Europene vizate modalități de alocare și rambursare a costurilor.
Articolul 74. Notificări (1) Statele membre notifică agenției eu-LISA autoritățile competente menționate la articolul 36. Respectivetele autorități pot utiliza routerul sau pot avea acces la acesta.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 53. Notificări (1) Punctul național de contact notifică Agenția eu-LISA lista autorităților competente, autorizate să utilizeze Routerul ori să aibă acces la acesta în scopul căutării și schimbului de profiluri ADN, date dactiloscopice și imagini faciale. (2) Orice modificare privind lista autorităților naționale autorizate să acceseze Routerul, precum și actualizarea profilurilor de acces ale membrilor personalului autorizat, se comunică Agenției eu-LISA fără întârzieri nejustificate.
(2) eu-LISA notifică Comisiei finalizarea cu succes a testării menționate la articolul 75 alineatul (1) litera (b).		Prevedere UE neaplicabilă	Prevederea stabilește notificarea între eu-LISA și Comisie relație instituțională UE.
(3) Europol notifică Comisiei finalizarea cu succes a testării menționate la articolul 75 alineatul (3) litera (b).		Prevedere UE neaplicabilă	Prevederea stabilește notificarea Europol-Comisie.
(4) Fiecare stat membru transmite celorlalte state membre, Comisiei, eu-LISA și Europol conținutul bazelor sale naționale de date ADN și condițiile pentru căutările automatizate cărora li se aplică articolele 5 și 6.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 53. Notificări (3) Autoritatea competentă informează celelalte state membre ale Uniunii Europene, Comisia

			Europeană, Agenția eu-LISA și Europol privind conținutul Registrului de stat al datelor genetice, precum și condițiile tehnice și juridice stabilite pentru efectuarea căutărilor automatizate de profiluri ADN.
(5) Fiecare stat membru informează celelalte state membre, Comisia, eu-LISA și Europol cu privire la conținutul bazelor sale de date dactiloscopice naționale și la condițiile pentru căutărilor automatizate cărora li se aplică articolele 10 și 11.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 53. Notificări (4) Autoritatea competentă informează celelalte state membre ale Uniunii Europene, Comisia Europeană, Agenția eu-LISA și Europol privind conținutul Registrului de stat dactiloscopic, precum și condițiile tehnice și juridice stabilite pentru efectuarea căutărilor automatizate de date dactiloscopice.
(6) Fiecare stat membru informează celelalte state membre, Comisia, eu-LISA și Europol cu privire la conținutul bazelor sale de date naționale privind imaginile faciale și la condițiile pentru căutărilor automatizate cărora li se aplică articolele 19 și 20.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 53. Notificări (5) Autoritatea competentă informează celelalte state membre ale Uniunii Europene, Comisia Europeană, Agenția eu-LISA și Europol privind conținutul bazei de date naționale privind imaginile faciale, precum și condițiile tehnice și juridice stabilite pentru efectuarea căutărilor automatizate de date ale imaginilor faciale.

(7) Statele membre care participă la schimburile automatizate de evidențe ale poliției în temeiul articolelor 25 și 26 transmit celorlalte state membre, Comisiei și Europol conținutul registrelor lor naționale de evidențe ale poliției și al bazelor naționale de date utilizate pentru stabilirea registrelor respective și condițiile pentru căutările automatizate.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 53. Notificări (6) În vederea participării la schimbul automatizat de evidențe ale poliției, autoritatea competentă informează celelalte state membre ale Uniunii Europene, Comisia Europeană, Agenția eu-LISA și Europol informații privind conținutul registrelor naționale de evidențe ale poliției, sursele de date utilizate pentru stabilirea acestora și criteriile stabilite pentru căutările automatizate prin sistemul EPRIS.
(8) Statele membre notifică Comisiei, eu-LISA și Europol punctul lor de contact național desemnat în temeiul articolului 30. Comisia întocmește o listă a punctelor de contact naționale care i-au fost notificate și o pune la dispoziția tuturor statelor membre.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 53. Notificări (7) Punctul unic de contact notifică oficial Comisia Europeană, Agenția eu-LISA și Europol identitatea și datele de legătură ale punctelor naționale de contact desemnate conform art. 6 și utilizează lista centralizată a punctelor naționale de contact, gestionată de Comisia Europeană, pentru coordonarea operativă a schimbului de date.
Articolul 75. Începerea funcționării (1) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care statele membre și Europol pot începe să		Prevedere UE neaplicabilă	Prevederea stabilește o competență exclusivă a Comisiei de a fixa data de utilizare pentru statele membre și Europol și

utilizeze routerul, după îndeplinirea următoarelor condiții: (a) măsurile prevăzute la articolul 5 alineatul (3), la articolul 8 alineatele (2) și (3), la articolul 13 alineatele (2) și (3), la articolul 17 alineatul (3), la articolul 22 alineatele (2) și (3), la articolul 31 și la articolul 37 alineatul (6) au fost adoptate; (b) eu-LISA a notificat finalizarea cu succes a unei testări complete a routerului, pe care a efectuat-o în cooperare cu autoritățile competente ale statelor membre și cu Europol. Comisia stabilește, prin intermediul actului de punere în aplicare menționat în primul paragraf, data de la care statele membre și Europol urmează să înceapă să utilizeze routerul. Respectiva dată este la un an de la data stabilită în conformitate cu primul paragraf. Comisia poate amâna cu cel mult un an data de la care statele membre și Europol urmează să înceapă să utilizeze routerul, în cazul în care o evaluare a implementării routerului a indicat că o astfel de amânare este necesară.			condiționează această dată de adoptarea unor măsuri UE și de notificarea testării de către eu-LISA, iar mecanismul de stabilire/amânare a datei de start este parte din procedurile UE.
(2) Statele membre asigură, la doi ani de la începerea funcționării routerului, disponibilitatea imaginilor faciale, astfel cum se menționează la articolul 19, în scopul căutării automatizate a imaginilor faciale, astfel cum se menționează la articolul 20.		Prevedere UE neaplicabilă	Prevedere stabilește că termenul este calculat/raportat la începerea funcționării routerului stabilită printr-un act al Comisiei UE pentru state membre.
(3) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care statele membre și Europol urmează să înceapă să utilizeze EPRIS, după îndeplinirea următoarelor condiții:		Prevedere UE neaplicabilă	Prevederea stabilește ca data de utilizare a EPRIS este stabilită tot de Comisia UE prin act de punere în aplicare, condiționată de măsuri

(a) măsurile prevăzute la articolul 44 alineatul (6) au fost adoptate; (b) Europol a notificat finalizarea cu succes a unei testări complete a EPRIS, pe care a efectuat-o în cooperare cu autoritățile competente ale statelor membre.			UE și de testare notificată de Europol
(4) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care Europol urmează să pună la dispoziția statelor membre datele biometrice provenite din țări terțe, în conformitate cu articolul 48, după îndeplinirea următoarelor condiții: (a) routerul este în funcțiune; (b) Europol a notificat finalizarea cu succes a unei testări complete a conexiunii sale cu routerul, pe care a efectuat-o în cooperare cu autoritățile competente ale statelor membre și cu eu-LISA.		Prevedere UE neaplicabilă	Prevederea stabilește un moment de la care Europol furnizează date către statele membre, după ce routerul e în funcțiune și după testarea conexiunii Europol-router împreună cu eu-LISA, fiind un flux intern al UE
(5) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care Europol urmează să aibă acces la datele stocate în bazele de date ale statelor membre în conformitate cu articolul 49, după îndeplinirea următoarelor condiții: (a) routerul este în funcțiune; (b) Europol a notificat finalizarea cu succes a unei testări complete a conexiunii sale cu routerul, pe care a efectuat-o în cooperare cu autoritățile competente ale statelor membre și cu eu-LISA.		Prevedere UE neaplicabilă	Prevederea reglementează data de la care Europol are acces la bazele de date ale statelor membre (condiționată de funcționarea routerului și testarea conexiunii), fiind o relație instituțională exclusiv UE.
(6) Actele de punere în aplicare menționate la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).		Prevedere UE neaplicabilă	Prevederea reglementează comitologia UE (procedura de examinare) pentru actele Comisiei.
Articolul 76. Dispoziții tranzitorii și derogări		Prevedere UE neaplicabilă	Partea a doua a prevederii Comisia stabilește, prin

(1) Statele membre și agențiile Uniunii încep să aplice articolele 19-22, articolul 47 și articolul 49 alineatul (6) de la data stabilită în conformitate cu articolul 75 alineatul (1) primul paragraf, cu excepția statelor membre care nu au început să utilizeze routerul.			intermediul unui act de punere în aplicare, data de la care statele membre și Europol pot începe să utilizeze routerul ce țin de imaginile faciale.
(2) Statele membre și agențiile Uniunii încep să aplice articolele 25-28 și articolul 49 alineatul (4) de la data stabilită în conformitate cu articolul 75 alineatul (3).		Prevedere UE neaplicabilă	Partea a doua a prevederii Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care statele membre și Europol urmează să înceapă să utilizeze EPRIS ce ține de evidențele poliției.
(3) Statele membre și agențiile Uniunii încep să aplice articolul 48 de la data stabilită în conformitate cu articolul 75 alineatul (4).		Prevedere UE neaplicabilă	Partea a doua a prevederii Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care Europol urmează să pună la dispoziția statelor membre datele biometrice provenite din țări terțe
(4) Statele membre și agențiile Uniunii încep să aplice articolul 49 alineatele (1), (2), (3), (5) și (7) de la data stabilită în conformitate cu articolul 75 alineatul (5).		Prevedere UE neaplicabilă	Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care Europol urmează să aibă acces la datele stocate în bazele de date ale statelor membre, respectiv interogările și accesul Europol la datele stocate în bazele de date ale statelor membre, utilizând datele furnizate de țări terțe.
Articolul 77. Procedura comitetului (1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.		Prevedere UE neaplicabilă	Comisia este asistată de un comitet în sensul Regulamentului (UE) nr. 182/2011, ca un mecanism de control al statelor membre asupra competențelor de executare ale actelor Comisiei.

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011. În cazul în care comitetul nu emite un aviz, Comisia nu adoptă proiectul de act de punere în aplicare și se aplică articolul 5 alineatul (4) al treilea paragraf din Regulamentul (UE) nr. 182/2011.		Prevedere UE neaplicabilă	Prevederea instituie o procedură UE de adoptare a actelor de punere în aplicare.
Articolul 78. Grupul consultativ pentru interoperabilitate Responsabilitățile Grupului consultativ pentru interoperabilitate instituit prin articolul 75 din Regulamentul (UE) 2019/817 și articolul 71 din Regulamentul (UE) 2019/818 se extind pentru a include routerul. Grupul consultativ pentru interoperabilitate furnizează eu-LISA cunoștințele de specialitate legate de router, în special în contextul pregătirii programului său de lucru anual și al raportului său anual de activitate.		Prevedere UE neaplicabilă	Prevederea extinde atribuțiile unui grup consultativ instituit prin regulamente UE (2019/817 și 2019/818) și stabilește rolul acestuia în raport cu eu-LISA (agenție UE) pentru router (program de lucru anual, raport anual).
Articolul 79. Manual practic Comisia, în strânsă cooperare cu statele membre, cu eu-LISA, cu Europol și cu Agenția pentru Drepturi Fundamentale a Uniunii Europene, pune la dispoziție un manual practic pentru punerea în aplicare și gestionarea prezentului regulament. Manualul practic furnizează orientări, recomandări și bune practici cu caracter tehnic și operațional. Comisia adoptă manualul practic sub forma unei recomandări înainte de începerea funcționării routerului și a EPRIS. Comisia actualizează manualul practic periodic și acolo unde este necesar.		Prevedere UE neaplicabilă	Prevederea obligă Comisia UE (împreună cu statele membre, eu-LISA, Europol și Agenția UE pentru Drepturi Fundamentale) să elaboreze și să adopte un manual sub forma unei recomandări UE, înainte de începerea funcționării routerului/EPRIS, și să-l actualizeze.
Articolul 80. Monitorizare și evaluare (1) eu-LISA se asigură că există proceduri pentru a monitoriza dezvoltarea routerului din		Prevedere UE neaplicabilă	Prevederea repartizează sarcini de monitorizare, raportare și evaluare către eu-LISA, Europol și

perspectiva obiectivelor legate de planificare și costuri și pentru a monitoriza funcționarea sa din perspectiva obiectivelor legate de realizările tehnice, de raportul cost-eficiență, de securitate și de calitatea serviciilor. Europol se asigură că există proceduri pentru a monitoriza dezvoltarea EPRIS din perspectiva obiectivelor legate de planificare și costuri și pentru a monitoriza funcționarea sa din perspectiva obiectivelor legate de realizările tehnice, de raportul cost-eficiență, de securitate și de calitatea serviciilor.			Comisia UE, cu raportare către Parlamentul European/Consiliu/Comisie și alte organisme UE, cu termene/calendar UE și cu referințe la finanțarea din bugetul general al UE.
(2) Până la 26 aprilie 2025 și, ulterior, în fiecare an pe durata fazei de dezvoltare a routerului, eu-LISA prezintă Parlamentului European și Consiliului un raport privind stadiul dezvoltării routerului. Respectivul rapoarte conțin informații detaliate cu privire la costurile ocazionale, precum și informații despre riscurile care ar putea avea un impact asupra costurilor totale care urmează să fie suportate din bugetul general al Uniunii în temeiul articolului 73. După încheierea etapei de dezvoltare a routerului, eu-LISA transmite Parlamentului European și Consiliului un raport în care explică în detaliu modul în care au fost îndeplinite obiectivele, în special cele referitoare la planificare și costuri, și în care se justifică eventualele abateri.		Prevedere UE neaplicabilă	Prevederea repartizează sarcini de monitorizare, raportare și evaluare către eu-LISA, Europol și Comisia UE, cu raportare către Parlamentul European/Consiliu/Comisie și alte organisme UE, cu termene/calendar UE și cu referințe la finanțarea din bugetul general al UE.
(3) Până la 26 aprilie 2025 și, ulterior, în fiecare an în cursul etapei de dezvoltare a EPRIS, Europol prezintă Parlamentului European și Consiliului un raport privind stadiul dezvoltării EPRIS. Respectivul rapoarte conțin informații detaliate cu privire		Prevedere UE neaplicabilă	Prevederea repartizează sarcini de monitorizare, raportare și evaluare către eu-LISA, Europol și Comisia UE, cu raportare către Parlamentul European/Consiliu/Comisie și alte

la costurile ocazionate, precum și informații despre riscurile care ar putea avea un impact asupra costurilor totale care urmează să fie suportate din bugetul general al Uniunii în temeiul articolului 73. După încheierea etapei de dezvoltare a EPRIS, Europol transmite Parlamentului European și Consiliului un raport în care explică în detaliu modul în care au fost îndeplinite obiectivele, în special cele referitoare la planificare și costuri, și în care se justifică eventualele abateri.			organisme UE, cu termene/calendar UE și cu referințe la finanțarea din bugetul general al UE.
(4) În vederea întreținerii tehnice, eu-LISA are acces la informațiile necesare referitoare la operațiunile de prelucrare a datelor efectuate în router. În vederea întreținerii tehnice, Europol are acces la informațiile necesare referitoare la operațiunile de prelucrare a datelor efectuate în EPRIS.		Prevedere UE neaplicabilă	Prevederea repartizează sarcini de monitorizare, raportare și evaluare către eu-LISA, Europol și Comisia UE, cu raportare către Parlamentul European/Consiliu/Comisie și alte organisme UE, cu termene/calendar UE și cu referințe la finanțarea din bugetul general al UE.
(5) După doi ani de la începerea funcționării routerului și, ulterior, o dată la doi ani, eu-LISA prezintă Parlamentului European, Consiliului și Comisiei un raport privind funcționarea tehnică a routerului, inclusiv în ceea ce privește securitatea routerului.		Prevedere UE neaplicabilă	Prevederea repartizează sarcini de monitorizare, raportare și evaluare către eu-LISA, Europol și Comisia UE, cu raportare către Parlamentul European/Consiliu/Comisie și alte organisme UE, cu termene/calendar UE și cu referințe la finanțarea din bugetul general al UE.
(6) După doi ani de la începerea funcționării EPRIS și, ulterior, o dată la doi ani, Europol prezintă Parlamentului European, Consiliului și Comisiei un raport		Prevedere UE neaplicabilă	Prevederea repartizează sarcini de monitorizare, raportare și evaluare către eu-LISA, Europol și Comisia UE, cu raportare către

privind funcționarea tehnică a EPRIS, inclusiv în ceea ce privește securitatea EPRIS.			Parlamentul European/Consiliu/Comisie și alte organisme UE, cu termene/calendar UE și cu referințe la finanțarea din bugetul general al UE.
(7) După trei ani de la punerea în funcțiune a routerului și a EPRIS, astfel cum se prevede la articolul 75 și, ulterior, o dată la patru ani, Comisia prezintă un raport de evaluare globală a cadrului Prüm II. După un an de la punerea în funcțiune a routerului și, ulterior, o dată la doi ani, Comisia prezintă un raport de evaluare globală a utilizării imaginilor faciale în temeiul prezentului regulament. Rapoartele menționate la primul și al doilea paragraf includ următoarele: (a) o analiză a aplicării prezentului regulament, inclusiv utilizarea lui de către fiecare stat membru și Europol; (b) o examinare a rezultatelor obținute în raport cu obiectivele prezentului regulament și a impactului său asupra drepturilor fundamentale; (c) impactul, eficacitatea și eficiența activității cadrului Prüm II și ale practicilor sale de lucru având în vedere obiectivele, mandatul și atribuțiile sale; (d) o evaluare a gradului de securitate al cadrului Prüm II. Comisia transmite rapoartele respective Parlamentului European, Consiliului, Autorității Europene pentru Protecția Datelor și Agenției pentru Drepturi Fundamentale a Uniunii Europene.		Prevedere UE neaplicabilă	Prevederea repartizează sarcini de monitorizare, raportare și evaluare către eu-LISA, Europol și Comisia UE, cu raportare către Parlamentul European/Consiliu/Comisie și alte organisme UE, cu termene/calendar UE și cu referințe la finanțarea din bugetul general al UE.

(8) În rapoartele menționate la alineatul (7) primul paragraf, Comisia acordă o atenție deosebită următoarelor noi categorii de date: imaginile faciale și evidențele poliției. Comisia include în astfel de rapoarte utilizarea de către fiecare stat membru și Europol a respectivelor noi categorii de date și impactul, eficacitatea și eficiența acestora. În rapoartele menționate la alineatul (7) al doilea paragraf, Comisia acordă o atenție deosebită riscului de concordanțe false și calității datelor.		Prevedere UE neaplicabilă	Prevederea repartizează sarcini de monitorizare, raportare și evaluare către eu-LISA, Europol și Comisia UE, cu raportare către Parlamentul European/Consiliu/Comisie și alte organisme UE, cu termene/calendar UE și cu referințe la finanțarea din bugetul general al UE.
(9) Statele membre și Europol furnizează eu-LISA și Comisiei informațiile necesare pentru elaborarea rapoartelor menționate la alineatele (2) și (5). Respectivile informații nu trebuie să pericliteze metodele de lucru și nici să dezvăluie sursele, membrii personalului sau investigațiile autorităților competente din statele membre.		Prevedere UE neaplicabilă	Prevederea repartizează sarcini de monitorizare, raportare și evaluare către eu-LISA, Europol și Comisia UE, cu raportare către Parlamentul European/Consiliu/Comisie și alte organisme UE, cu termene/calendar UE și cu referințe la finanțarea din bugetul general al UE.
(10) Statele membre transmit Comisiei și Europol informațiile necesare pentru elaborarea rapoartelor prevăzute la alineatele (3) și (6). Respectivile informații nu trebuie să pericliteze metodele de lucru și nici să dezvăluie sursele, membrii personalului sau investigațiile autorităților competente din statele membre.		Prevedere UE neaplicabilă	Prevederea repartizează sarcini de monitorizare, raportare și evaluare către eu-LISA, Europol și Comisia UE, cu raportare către Parlamentul European/Consiliu/Comisie și alte organisme UE, cu termene/calendar UE și cu referințe la finanțarea din bugetul general al UE.
(11) Fără a aduce atingere cerințelor în materie de confidențialitate, statele membre, eu-LISA și Europol furnizează Comisiei informațiile necesare pentru realizarea rapoartelor menționate la alineatul (7). De		Prevedere UE neaplicabilă	Prevederea repartizează sarcini de monitorizare, raportare și evaluare către eu-LISA, Europol și Comisia UE, cu raportare către Parlamentul

asemenea, statele membre transmit Comisiei numărul de concordanțe confirmate în baza de date a fiecărui stat membru pentru fiecare categorie și pentru fiecare tip de date. Respectivle informații nu trebuie să pericliteze metodele de lucru și nici să dezvăluie sursele, membrii personalului sau investigațiile autorităților competente din statele membre.			European/Consiliu/Comisie și alte organisme UE, cu termene/calendar UE și cu referințe la finanțarea din bugetul general al UE.

TABEL DE CONCORDANȚĂ
a proiectului de lege privind cooperarea polițienească internațională

1.	Titlul actului UE, inclusiv cea mai recentă modificare, nr. CELEX: 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			
2.	Titlul proiectului de act normativ național: Proiect de Hotărâre 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			
3.	Gradul general de compatibilitate Parțial compatibil			
4.	Autoritatea/persoana responsabilă Ministerul Afacerilor Interne			
5.	Data întocmirii/actualizării 15.05.2026			
6. Actul Uniunii Europene		7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observații
Articolul 1. Definiții În sensul prezentei decizii, se aplică următoarele definiții: 1. „Vehicul” înseamnă orice autovehicul, remorcă sau rulotă, în conformitate cu definiția din dispozițiile referitoare la Sistemul de Informații Schengen (SIS).			Compatibil	<i>Legea nr. 131/2007 privind siguranța traficului rutier</i> Art. 2 Noțiuni principale: <i>vehicul</i> – sistem mecanic, cu sau fără autoproulsie, destinat transportului de persoane sau de bunuri ori echipat cu mecanisme care pot executa anumite lucrări. <i>Legea nr. 106/2022 privind asigurarea obligatorie de răspundere civilă auto pentru pagube produse de vehicule</i> Art. 3 Noțiuni principale: <i>vehicul</i> – sistem mecanic, cu sau fără autoproulsie, destinat transportului de persoane sau de bunuri ori echipat cu mecanisme care pot executa anumite lucrări, dar care nu se deplasează pe șine,

			inclusiv orice tip de remorcă, indiferent dacă este cuplată sau nu, pentru care în Republica Moldova există obligația legală de înmatriculare. Regulamentul circulației rutiere aprobat prin Hotărârea Guvernului nr. 357/2009 pct. 7. În sensul prezentului Regulament următoarele noțiuni și termeni semnifică: <i>vehicul</i> – sistem mecanic, cu sau fără autopropulsie, destinat transportului de persoane și bunuri sau echipat cu mecanisme care pot executa anumite lucrări;
2. „Autorități naționale competente” înseamnă orice autorități naționale desemnate de statele membre în sensul prezentei decizii și pot include, după caz, poliția, administrația vamală, polițiștii de frontieră și autoritățile judiciare.		Compatibil	Proiectul de lege privind cooperarea polițienească internațională Articolul 3. Noțiuni principale 1) <i>autoritate competentă</i> – autoritate publică, instituție sau altă entitate abilitată prin lege să exercite atribuții în domeniile reglementate de prezenta lege. 2) <i>autoritate competentă de aplicare a legii</i> – autoritate polițienească, judiciară, vamală sau altă autoritate de aplicare a legii, din Republica Moldova sau din alte țări, cu atribuții în prevenirea, depistarea sau investigarea infracțiunilor.
Articolul 2. Obiectiv (1) Prezenta decizie are ca obiectiv realizarea unei mai bune cooperări în cadrul Uniunii Europene, în scopul prevenirii și combaterii criminalității transfrontaliere referitoare la vehicule.		Compatibil	Proiectul de lege privind cooperarea polițienească internațională Articolul 1. Obiectul de reglementare (2) Prezenta lege stabilește norme privind: b) schimbul de date cu privire la căutarea directă sau automatizată de

			profiluri ADN, date dactiloscopice, date privind vehicule precum și piesele componente ale acestuia consemnate cu număr de identificare, imagini faciale, date privind documente de călătorie declarate furate, pierdute, revocate, nevalidate sau blancurile documentelor furate înainte de emitere, evidențe ale poliției, datele personale ale persoanelor străine sau cetățenilor Republicii Moldova urmăriți internațional, aflați în vizorul autorităților de aplicare a legii, datele biometrice și antropometrice necesare identificării persoanelor dispărute fără veste, cadavrelor și părților acestuia, precum și alte date care fac obiectul schimbului de date de interes polițienesc;
(2) O atenție deosebită se acordă relației între furtul de vehicule și comerțul ilegal cu vehicule și alte forme de criminalitate organizată, precum traficul de droguri, de arme de foc și de persoane.		Compatibil	<i>Hotărârea Guvernului nr. 1145/2018 cu privire la organizarea și funcționarea Inspectoratului General al Poliției de Frontieră</i> Anexa nr. 2 Structura IGPF prevede Secția combaterea traficului ilicit de droguri, Secția combaterea migrației ilegale și a traficului de ființe umane, Secția combaterea contrabandei în cadrul Direcției investigare criminalitate transfrontalieră. <i>Legea nr. 50/2012 privind prevenirea și combaterea criminalității organizate</i> Articolul 18 Cooperarea și asistența internațională (1) Cooperarea internațională în domeniul prevenirii și combaterii criminalității organizate se desfășoară prin

			schimb de informații între serviciile naționale și internaționale interesate, prin acordare de asistență juridică în materie penală, inclusiv prin comisii rogatorii, sau prin alte activități necesare pentru prevenirea și combaterea criminalității organizate, în conformitate cu legislația națională și internațională, fără prejudicierea drepturilor și libertăților fundamentale ale omului.
Articolul 3. Cooperarea între autoritățile naționale competente (1) Statele membre iau măsurile necesare, în conformitate cu legislația internă, pentru a îmbunătăți cooperarea dintre autoritățile naționale competente, în scopul combaterii criminalității transfrontaliere referitoare la vehicule, în special prin intermediul acordurilor de cooperare.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Regulamentului cu privire la registrul de stat al vehiculelor, aprobat prin Hotărârea de Guvern nr. 1047/1999.</i>
(2) O atenție specială se acordă cooperării referitoare la controlul exporturilor, luând în considerare diferitele competențe din statele membre.		Compatibil	<i>Legea nr. 283/2011 cu privire la Poliția de Frontieră</i> Articolul 6 Atribuțiile Poliției de Frontieră (1) în domeniul supravegherii și controlului trecerii frontierei de stat, Poliția de Frontieră: d) asigură evidență, inclusiv automatizată, a persoanelor și mijloacelor de transport care au traversat frontiera de stat; <i>Legea nr. 302/2017 cu privire la Serviciul Vamal</i> Articolul 7 Misiunea și funcțiile de bază

			f) efectuarea controlului și a supravegherii vamale, inclusiv prevenirea, depistarea și combaterea contrabandei și a eschivării de la achitarea drepturilor de import/export și a altor plăți;
Articolul 4. Cooperarea între autoritățile competente și sectorul privat (1) Statele membre iau măsurile necesare pentru a organiza consultări periodice, după caz, între autoritățile naționale competente, în conformitate cu legislația internă, putând implica și reprezentanți ai sectorului privat (precum responsabili cu registrele private ale vehiculelor dispărute, asigurători și reprezentanți ai sectorului de comerț cu autovehicule) în astfel de consultări, în vederea coordonării informațiilor și alinierii reciproce a activităților în acest domeniu.		Compatibil	<i>Legea nr.106/2022 privind asigurarea obligatorie de răspundere civilă auto pentru pagube produse de vehicule</i> Articolul 23 Informația despre accident (1) Instituțiile subordonate ale Ministerului Afacerilor Interne, organele de drept și instanțele judecătorești, instituțiile medicale și alte persoane juridice de drept public și privat, care dispun de informațiile necesare pentru instrumentarea dosarului de daune sau pentru exercitarea dreptului de regres al asigurătorului RCA, prezintă, în mod obligatoriu, asiguratului și/sau persoanei păgubite documente și date, pe suport de hârtie, în formă electronică ori cu convertirea documentației respective într-un format electronic ușor accesibil, inclusiv cu utilizarea semnăturii electronice simple, în mod gratuit și în termen de 15 zile lucrătoare, la cererea asigurătorului RCA. În cazul în care informația necesară se regăsește în Registrul de stat al accidentelor rutiere, aceasta este obținută de către asigurătorul RCA prin intermediul platformei de interoperabilitate (MConnect), direct din registrul menționat. (2) Ministerul Afacerilor Interne, „Agenția Servicii Publice” și Agenția

		Națională Transport Auto prezintă informațiile necesare pentru buna funcționare a Sistemului informațional automatizat de stat în domeniul asigurărilor obligatorii RCA în mod continuu și în timp util. <i>Legea nr. 320/2012 cu privire la activitatea Poliției și statutul polițistului</i> Articolul 6 Cooperarea Poliției cu alte organe de drept, autorități ale administrației publice centrale și locale, cu mass-media, societatea civilă și cu organisme internaționale (2) Poliția cooperează cu autorități ale administrației publice centrale și locale în vederea realizării atribuțiilor sale, prevederilor documentelor de politici naționale în domeniul de prevenire și combatere a infracționalității, de menținere a ordinii și securității publice, implicând în aceste activități și societatea civilă. (3) Poliția cooperează cu societatea civilă, cu mass-media, precum și cu persoanele fizice și juridice, în modul stabilit de legislație și de actele normative ale Ministerului Afacerilor Interne. <i>Legea nr.302/2017 cu privire la Serviciul Vamal</i> Art. 5 Structura și efectivul-limită (5) Serviciul Vamal creează comitetul consultativ, care este un organ consultativ de facilitare a comerțului internațional și care are drept scop promovarea unui

			dialog și a unui parteneriat între Serviciul Vamal și comunitatea de afaceri, în vederea asigurării transparenței și implementării celor mai bune practici internaționale în domeniul vamal. Organizarea, funcționarea, componența și modul de luare a deciziilor în cadrul comitetului consultativ se stabilesc printr-un regulament aprobat prin ordinul directorului Serviciului Vamal.
(2) Statele membre simplifică procedurile, în conformitate cu legislația internă, în vederea unei repatrieri rapide a vehiculelor restituite de autoritățile naționale competente după sechestrarea acestora.		Compatibil	<i>Cod nr. 122/2003 de procedură penală al Republicii Moldova</i> Articolul 161 Hotărârea cu privire la corpurile delictelor adoptată până la soluționarea cauzei penale (1) Până la soluționarea cauzei penale, procurorul ori ofițerul de urmărire penală care are încuviințarea procurorului, în faza urmăririi penale, sau, după caz, instanța dispune restituirea către proprietarul sau posesorul legal: 4) a automobilului sau a unui alt mijloc de transport, dacă acesta nu a fost sechestrat pentru asigurarea acțiunii civile în cauza penală sau a posibilei confiscări speciale a bunurilor. <i>Legea nr.371/2006 cu privire la asistență juridică internațională în materie penală</i> Articolul 12 Remiterea de obiecte și de alte valori (1) În cazul în care cererea de asistență juridică are ca obiect sau implică remiterea de obiecte sau de alte valori, acestea pot fi predate atunci când nu sînt

			necesare dovedirii unei fapte penale ale cărei urmărire și judecată țin de atribuțiile autorităților competente ale Republicii Moldova. (5) În cazul cererilor de extrădare, predarea obiectelor și altor valori prevăzute la alin.(1) se poate efectua chiar dacă nu se acordă extrădarea, în special din cauza evadării sau decesului persoanei a cărei extrădare se cere. Proiectul de lege privind cooperarea polițienească internațională: Articolul 16. Cooperarea internațională privind vehiculele furate, răpite sau însușite ilegal (3) În cazul identificării pe teritoriul Republicii Moldova a unui vehicul semnalat de alt stat ca fiind furat, răpit sau dobândit ilegal, autoritatea competentă de aplicare a legii, prin intermediul punctului național de contact: a) informează fără întârziere statul care a introdus semnalarea; b) dispune măsurile prevăzute de lege pentru indisponibilizarea vehiculului; c) cooperează, în condițiile legii, în vederea clarificării situației juridice și, după caz, a restituirii vehiculului către persoana îndreptățită.
Articolul 5. Puncte de contact pentru combaterea criminalității referitoare la vehicule (1) Până la 30 martie 2005, statele membre desemnează, în cadrul autorităților lor de aplicare a legii, un	<i>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</i>	Compatibil	Proiectul de lege privind cooperarea polițienească internațională Articolul 6. Punctul unic de contact și atribuțiile acestuia (1) Se desemnează în calitate de punct unic de contact pentru cooperarea

punct de contact pentru combaterea criminalității transfrontaliere referitoare la vehicule.	Anexa nr. 2 Punctul 4. În sensul prezentului Regulament, se desemnează următoarele autorități în calitate de PNC, responsabile de gestionarea bazelor de date naționale și furnizarea informațiilor către PUC: 4.4. <i>Agenția Servicii Publice (în continuare – ASP)</i> — pentru domeniul de date privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, date privind documente de călătorie, vizele, titlurile de valoare, inclusiv a celor declarate false, furate sau pierdute, precum și date privind permisele de conducere;		polițienească internațională subdiviziunea specializată în cooperare polițienească internațională din subordinea Inspectoratului General al Poliției al Ministerului Afacerilor Interne. (2) Punctul unic de contact asigură cooperarea cu punctele naționale de contact desemnate prin hotărâre de Guvern, din cadrul autorităților competente naționale, pe următoarele domenii: c) date referitoare la mijloace de transport, inclusiv autovehicule anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale; (7) Organizarea, funcțiile și modul de funcționare a punctului unic de contact și a punctelor naționale de contact pe domeniile prevăzute la alin. (2), se stabilesc prin hotărâre de Guvern.
(2) Statele membre autorizează punctele de contact să facă schimb de experiență, de cunoștințe de specialitate, precum și de informații generale și tehnice privind criminalitatea referitoare la vehicule, în baza legislației aplicabile existente. Schimbul de informații se extinde asupra metodelor și asupra celor mai bune practici de prevenire a criminalității referitoare la vehicule. Astfel de schimburi nu includ schimburile de date cu caracter personal.	<i>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</i> Anexa nr.1 Punctul 12. În scopul consolidării cooperării polițienești internaționale, conducătorul PUC are următoarele responsabilități de coordonare internațională: 12.5. facilitează schimbul de experiență, de cunoștințe de specialitate,	Compatibil	

	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.		
(3) Informațiile privind punctele naționale de contact desemnate, inclusiv modificările ulterioare, se comunică Secretariatului General al Consiliului pentru publicarea în Jurnalul Oficial al Uniunii Europene.	<i>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</i> Anexa nr.1 Punctul 10. PUC acționează ca interfață unică și acționează ca interfață unică și centralizată între sistemele informaționale naționale și infrastructura centrală a Uniunii Europene, fiind structura administrativă și operațională desemnată la nivel național pentru a asigura fluxul informațional securizat cu statele membre ale Uniunii Europene, alte state și organizațiile internaționale profilate pe schimbul de date și informații de natură infracțională, având următoarele atribuții funcționale și operaționale principale: 10.1 asigurarea notificării oficiale către Secretariatul General al Consiliului Uniunii Europene și Comisiei Europene, în termen de cel mult o lună de la data desemnării, cu privire la desemnarea PUC și a Punctelor Naționale de Contact (în continuare – PNC) pe domenii de competență, precum și a listei limbilor stabilite pentru schimbul de	Compatibil	

	informații conform pct. 39, inclusiv a oricăror modificări ulterioare ale acestora, în vederea publicării în Jurnalul Oficial al Uniunii Europene sau pe platformele online dedicate ale Comisiei;		
Articolul 6. Semnalarea furturilor de vehicule și a certificatelor de înmatriculare (1) Ori de câte ori se raportează furtul unui vehicul, autoritățile competente ale statelor membre introduc imediat o alertă de vehicul furat în SIS, în conformitate cu legislația internă și, atunci când este posibil, în baza de date a Interpol referitoare la autovehiculele furate.	<i>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</i> Anexa nr. 2 Punctul 62. ASP este desemnată în calitate de PNC responsabil de gestionarea bazelor de date naționale privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, a datelor referitoare la documente de călătorie, vizele, titlurile de valoare, 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. Punctul 65. ASP asigură interfața tehnică și fluxul de date necesar pentru	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 16. Cooperarea internațională privind vehiculele furate sau însușite ilegal (2) În cazul în care un vehicul înregistrat în Registrul de stat al vehiculelor este radiat din evidență, declarat furat, răpit, însușit ilegal sau constituie obiect al unei infracțiuni, autoritatea competentă: a) completează fără întârziere datele relevante în bazele de date naționale și în sistemele internaționale aplicabile; b) asigură actualizarea, rectificarea sau radierea semnalării, după caz; c) transmite, prin punctul național de contact, autorităților competente ale statelor membre, informațiile necesare care confirmă faptul că vehiculul se află sau a fost transferat pe teritoriul acestora; d) informează EUROPOL și INTERPOL despre autorii infracțiunilor referitoare la vehicule.

	introducerea și gestionarea în Sistemul de Informații Schengen (SIS) a alertelor referitoare la mijloacele de transport și documente (de călătorie, certificate de înmatriculare și permise de conducere) raportate ca fiind furate, pierdute, sustrase sau anulate.		
(2) Statul membru care a introdus alerta o retrage din registrul de căutare, în conformitate cu legislația internă, de îndată ce motivul de introducere a alertei asupra vehiculului încetează să mai existe.	<i>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</i> Anexa nr. 2 Punctul 68. 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/Biroului național SIRENE pentru actualizarea corespunzătoare în Sistemul de Informații Schengen.	Compatibil	
(3) Ori de câte ori se raportează furtul certificatelor de înmatriculare, autoritățile competente ale statelor membre introduc imediat o alertă în SIS, în conformitate cu legislația internă.	<i>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</i> Anexa nr. 2 Punctul 63. 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 (SIS) în toate cazurile de	Compatibil	

	raportare a furtului certificatelor de înmatriculare a vehiculelor.		
Articolul 7. Înmatriculare (1) Fiecare stat membru se asigură că autoritățile sale competente iau măsurile necesare pentru a preveni utilizarea frauduloasă și furtul de documente de înmatriculare a vehiculelor.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Regulamentului cu privire la registrul de stat al vehiculelor, aprobat prin Hotărârea de Guvern nr. 1047/1999.</i>
(2) Autoritățile de aplicare a legii informează autoritățile naționale de înmatriculare a vehiculelor în cazul se cunoaște că un vehicul, aflat în curs de înmatriculare, a fost furat. Accesul, în acest scop, la bazele de date se face în conformitate cu dispozițiile dreptului comunitar.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui <i>proiect de modificare a Regulamentului cu privire la registrul de stat al vehiculelor, aprobat prin Hotărârea de Guvern nr. 1047/1999.</i>
Articolul 8. Prevenirea utilizării frauduloase a certificatelor de înmatriculare a vehiculelor (1) Pentru a preveni utilizarea frauduloasă a certificatelor de înmatriculare a vehiculelor, fiecare stat membru se asigură, în conformitate cu legislația internă, că autoritățile sale competente iau măsurile necesare pentru a li se preda certificatul de înmatriculare al proprietarului vehiculului sau al deținătorului vehiculului, în cazul în care vehiculul a fost avariat grav într-un accident (pierdere totală).		Compatibil	<i>Legea nr.106/2022 privind asigurarea obligatorie de răspundere civilă auto pentru pagube produse de vehicule</i> Articolul 18 Obligațiile asiguratului (1) În cazul producerii accidentului de vehicul, asiguratul este obligat: b) să notifice organele de poliție sau alte organe de drept despre accidentul de vehicul (cu excepția accidentelor pasibile de documentarea prin procedura de constatare amiabilă a accidentului) imediat după producerea acestuia, solicitând întocmirea actelor referitoare la cauzele și circumstanțele producerii accidentului de vehicul, precum și la consecințele acestuia <i>Regulamentul cu privire la registrul de stat al vehiculelor, aprobat prin</i>

		<i>Hotărârea Guvernului nr. 1047/1999 cu privire la reorganizarea Sistemului informațional automatizat de căutare „Automobilul” în Registrul de stat al vehiculelor și introducerea testării a autovehiculelor și remorcilor acestora</i> Anexa nr. 2 Punctul 57 Proprietarii de vehicule înmatriculate pot solicita retragerea din circulație, dacă fac dovada depozitării acestora în afara domeniului public. Punctul 58 Radierea vehiculelor se face de către autoritatea care a efectuat înmatricularea, la cererea proprietarului, în următoarele cazuri: a) proprietarul sau mandatarul face dovada dezmembrării, casării sau predării vehiculului la unități specializate; b) vehiculul urmează să fie scos definitiv din Republica Moldova; Punctul 59. Vehiculul declarat prin hotărâre judecătorească fără stăpân sau abandonat se radiază din oficiu în termen de 30 de zile de la data când hotărârea a devenit definitivă. Punctul 60 Radierea se face pe baza depunerii certificatului de înmatriculare și a plăcilor cu număr de înmatriculare, precum și a documentelor care atestă faptul că a intervenit una dintre situațiile prevăzute la pct.58. Pentru vehiculele exportate din Republica Moldova, pe lângă certificatele de înmatriculare, se eliberează certificatele de înmatriculare provizorii și plăcile cu număr de înmatriculare tranzit. La radierea

			vehiculelor din evidență, în <u>certIFICATELE de înmatriculare se taie unghiul de sus din partea locului amplasării codului bidimensional.</u> Punctul 61 În cazul exportului din țară a vehiculelor procurate de către persoanele străine, se eliberează certificatul de înmatriculare provizoriu și plăcile cu număr de înmatriculare tranzit valabile pentru 30 de zile. Punctul 62 În cazul vehiculelor înmatriculate anterior datei de 1 ianuarie 1993, care dețin certificate de înmatriculare și numere de înmatriculare modele vechi sau care au o vechime de fabricație mai mare de 25 de ani, radierea se poate efectua în baza unei declarații pe propria răspundere a titularului înmatriculării ori a moștenitorilor legali sau testamentari ai acestuia, care să ateste că vehiculul a fost dezmembrat sau retras definitiv din circulație și nu mai circulă pe drumurile publice.
(2) De asemenea, un certificat de înmatriculare se predă, în conformitate cu legislația internă, în cazul în care, în timpul unui control efectuat de serviciul de aplicare a legii, se suspectează că a avut loc o fraudă cu privire la elementele de identificare a vehiculului, precum numărul de identificare al vehiculului.		Parțial compatibil	<i>Regulamentul cu privire la registrul de stat al vehiculelor, aprobat prin Hotărârea Guvernului nr. 1047/1999 cu privire la reorganizarea Sistemului informațional automatizat de căutare „Automobilul” în Registrul de stat al vehiculelor și introducerea testării a autovehiculelor și remorcilor acestora</i> Punctul 28 În cazul existenței unor indicii cu privire la falsificarea documentelor prevăzute la pct. 23 sau 26, se vor efectua verificări prin intermediul structurilor specializate ale Ministerului

			Afacerilor Interne cu competențe în domeniu, la solicitarea subdiviziunilor teritoriale de examinare și evidență a vehiculelor. Este interzisă înmatricularea vehiculelor în cazul constatării falsificărilor în datele înscrise în documentele de înmatriculare eliberate de autoritățile străine.
(3) Certificatele de înmatriculare se restituie doar în urma examinării și verificării pozitive a identității vehiculului și în conformitate cu legislația internă.		Parțial compatibil	<i>Regulamentul cu privire la registrul de stat al vehiculelor, aprobat prin Hotărârea Guvernului nr. 1047/1999 cu privire la reorganizarea Sistemului informațional automatizat de căutare „Automobilul” în Registrul de stat al vehiculelor și introducerea testării a autovehiculelor și remorcilor acestora</i> Punctul 18 Înmatricularea, cu excepția înmatriculării provizorii pentru probe, și eliberarea unui nou certificat de înmatriculare ca urmare a modificării unor date înscrise în acesta se face numai pentru autovehiculele și remorcile identificate și verificate de către un expert în identificarea vehiculelor, în sarcina căruia intră: a) atestarea faptului că principalele elemente de identificare ale vehiculului (numărul caroseriei, numărul șasiului și numărul motorului) sunt originale și/sau nu au fost supuse unor modificări neautorizate; b) atestarea identității vehiculului în raport cu datele menționate în certificatul de înmatriculare al acestuia; c) atestarea faptului că formularul-tip al documentului care confirmă

		înmatricularea anterioară a vehiculului, eliberat de autoritățile competente din țara de proveniență, este autentic (numai pentru vehiculele prezentate pentru prima înmatriculare în Republica Moldova). Punctul 23 Înmatricularea permanentă sau înmatricularea temporară se efectuează în baza următoarelor documente: f) documentul vamal care atestă importul definitiv sau temporar pentru înmatricularea temporară, în cazul autovehiculelor și al remorcilor importate în Republica Moldova, în original și în copie; h) procura, după caz; i) raportul de identificare a vehiculului. Punctul 23¹ Înmatricularea vehiculelor în conformitate cu prevederile Legii nr. 170/2018 cu privire la înmatricularea unor mijloace de transport și modificarea unor acte legislative, cu eliberarea certificatului de înmatriculare și a numerelor de înmatriculare neutre, se efectuează în baza următoarelor documente: e) certificatul de înmatriculare al vehiculului; f) documentul care atestă dreptul de proprietate al solicitantului asupra autovehiculului sau remorcii; i) raportul de identificare a vehiculului;

			j) documentul vamal care atestă importul vehiculului – în cazul vehiculelor importate după 24 aprilie 2018; k) actele de înmatriculare eliberate de autoritățile statelor străine – în cazul vehiculului care a mai fost înmatriculat în alt stat și care se înmatriculează pentru prima dată la autoritățile din Republica Moldova.
Articolul 9. Europol Fiecare stat membru se asigură că autoritățile sale de aplicare a legii informează Europol, după caz, în cadrul mandatului și misiunilor sale respective, cu privire la autorii infracțiunilor referitoare la vehicule.	<i>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</i> Anexa nr. 2 Punctul 66. 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.	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 16. Cooperarea internațională privind vehiculele radiate din evidență, furate sau însușite ilegal (2) În cazul în care un vehicul înregistrat în Registrul de stat al vehiculelor este radiat din evidență, declarat furat, răpit, însușit ilegal sau constituie obiect al unei infracțiuni, autoritatea competentă: d) informează EUROPOL și INTERPOL despre autorii infracțiunilor referitoare la vehicule. Cooperarea cu Europol Republica Moldova cooperează cu Oficiul European de Poliție (Europol) în baza Acordului Strategic de Cooperare semnat în 2007 și Acordului Operațional de Cooperare semnat la 18 decembrie 2014, la Chișinău. Din 2013, Republica Moldova a detașat un ofițer de legătură la Europol. <i>Sursa:</i> https://mfa.gov.md/ro/content/justitie-si-afaceri-interne

			Memorandumul de înțelegere între Republica Moldova și Oficiul European de Poliție privind linia securizată de comunicare din 16.01.2014 Regulamentul-cadru privind funcționarea Punctului Național de Contact va institui procedura specifică de notificare obligatorie a Europol.
Articolul 10. Promovarea cunoștințelor de specialitate și a formării profesionale Statele membre iau măsurile necesare pentru a se asigura că instituțiile naționale responsabile cu formarea profesională a respectivelor autorități de aplicare a legii promovează în programele lor de învățământ, atunci când este necesar în cooperare cu Colegiul European de Poliție, formarea profesională specializată în domeniul prevenirii și descoperirii criminalității referitoare la vehicule. O astfel de formare profesională poate cuprinde o contribuție din partea Europol, în conformitate cu domeniul său de competență.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 51. Responsabilitatea și instruirea (2) Autoritățile competente asigură, după caz, personalului autorizat implicat în aplicarea prezentei legi, resursele necesare și formarea profesională pentru îndeplinirea atribuțiilor. (3) Formarea prevăzută la alin. (2) include, în mod obligatoriu, instruirea privind: a) protecția datelor cu caracter personal și securitatea informației în cadrul schimbului de date realizat în temeiul prezentei legi; b) verificarea și confirmarea exactă a concordanțelor/rezultatelor obținute în urma căutărilor și comparațiilor efectuate, inclusiv prin proceduri de examinare manuală atunci când este cazul. Academia „Ștefan cel Mare” întreprinde măsurile și, în cadrul orelor la disciplina Drept penal, Partea specială, la tema „Infrațiuni în domeniul

			transporturilor” apare ca unitate de conținut infracțiunea de falsificare a elementelor de identificare ale autovehiculelor (art.276 CP), iar la tema „Infracțiuni contra bunei desfășurări a activității în sfera publică” - infracțiunea de fals în acte publice (art.332 CP). Totodată, formarea profesională în domeniul prevenirii și combaterii criminalității referitoare la vehicule se desfășoară la unitățile de curs orientate spre specializare. La programul de studii „Securitatea Frontierei” realizat în cadrul CIPAL, la modulele „Tactica controlului la trecerea Frontierei de Stat” și „Identificarea falsurilor în documentele de călătorie” se studiază subiecte care prevăd conținuturi din domeniul criminalității transfrontaliere și anume a furturilor de vehicule, a falsificării numerelor de identitate a vehiculelor și a documentelor de însoțire.
Articolul 11. Reuniunile punctelor de contact și raportul anual către Consiliu Punctele de contact pentru combaterea criminalității referitoare la vehicule se reunesc cel puțin o dată pe an, fiind prezidate de statul membru care deține președinția Consiliului. Europol este invitat să participe la respectiva reuniune. Președinția raportează Consiliului cu privire la progresele înregistrate în cadrul	<i>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</i> Anexa nr.1 12. În scopul consolidării cooperării polițienești internaționale, conducătorul PUC are următoarele responsabilități de coordonare internațională: 12.1 participă, cel puțin o dată pe an, la reuniunile organizate la nivelul Uniunii Europene cu șefii punctelor de	Compatibil	

cooperării practice relevante între autoritățile de aplicare a legii.	contact unice din celelalte state membre ale Uniunii Europene; 12.2 evaluează, în cadrul acestor reuniuni, calitatea cooperării dintre serviciile naționale și cele străine; 12.3 analizează și propune măsurile tehnice sau organizatorice necesare în cazul apariției unor dificultăți în schimbul de informații; 12.4 contribuie la clarificarea și armonizarea procedurilor operaționale de schimb de date și informații în conformitate cu standardele europene; 12.5 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.		
Articolul 12. Evaluare Consiliul evaluează punerea în aplicare a prezentei decizii până la 30 decembrie 2007.		Prevedere UE neaplicabilă	
Articolul 13. Intrarea în vigoare Prezenta decizie intră în vigoare la data publicării în Jurnalul Oficial al Uniunii Europene. Pentru acele state membre în care dispozițiile acquis-ului Schengen cu privire la SIS nu au intrat încă în vigoare, obligațiile prezentei decizii cu privire la SIS intră în vigoare la data la care începe aplicarea acestor dispoziții, după cum se menționează în decizia		Prevedere UE neaplicabilă	

Consiliului adoptată în acest sens în conformitate cu procedurile aplicabile.			

Tabel de concordanță

la proiectul de Hotărâre 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.	Titlul actului Uniunii Europene, inclusiv cele mai recentă modificare, nr. CELEX Titlul: Directiva (UE) 2023/977 a Parlamentului European și a Consiliului din 10 mai 2023 privind schimbul de informații între autoritățile de aplicare a legii ale statelor membre și de abrogare a Deciziei-cadru 2006/960/JAI a Consiliului.		
2.	Titlul proiectului de act normativ național Proiect de Hotărâre 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		
3.	Gradul general de compatibilitate Parțial compatibil		
4.	Autoritatea/persoana responsabilă Ministerul Afacerilor Interne		
5.	Data întocmirii/actualizării 18.05.2026		
6. Actul Uniunii Europene		7. Proiectul de act normativ național	8. Gradul de compatibilitate
Articolul 1. Obiect și domeniu de aplicare (1) Prezenta directivă stabilește norme armonizate privind schimbul adecvat și rapid de informații dintre autoritățile competente de aplicare a legii în scopul prevenirii, depistării sau investigării infracțiunilor. În special, prezenta directivă stabilește norme privind: (a) cererile de informații transmise punctelor de contact unice înființate sau desemnate de statele membre, în special cu privire la conținutul acestor cereri, furnizarea de informații în temeiul unor astfel de cereri, limbile de lucru ale punctelor de contact unice, termenele obligatorii pentru furnizarea informațiilor solicitate și motivele refuzului de a da curs unor astfel de cereri;		<i>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</i> Anexa nr.1 Punctul 2. Scopul prezentului Regulament este intensificarea cooperării polițienești internaționale pentru prevenirea, depistarea și investigarea infracțiunilor, precum și facilitarea căutării persoanelor dispărute și identificarea rămășițelor umane. Punctul 3. PUC își desfășoară activitatea în conformitate cu Legea privind cooperarea polițienească internațională și tratatele internaționale la care Republica Moldova este parte. Punctul 4. În scopul transunerii Directivei (UE) 2023/977, funcțiile de punct unic de contact pentru cooperarea polițienească internațională (<i>Single Point of Contact, în continuare – SPOC</i>) sunt exercitate de către PUC.	Compatibil Proiectul de lege privind cooperarea polițienească internațională Articolul 1. Obiectul de reglementare Prezenta lege stabilește cadrul juridic pentru consolidarea cooperării polițienești internaționale prin interogarea bazelor de date și schimbul de informații, inclusiv automatizat între autoritățile Republicii Moldova și autoritățile din statele membre ale Uniunii Europene și alte state, în special între autoritățile cu atribuții de prevenire, depistare și investigare a infracțiunilor, în condițiile tratatelor internaționale la care Republica Moldova este parte și ale actelor normative speciale aplicabile.

			Articolul 6. Punctul unic de contact și atribuțiile acestuia (1) Se desemnează în calitate de punct unic de contact pentru cooperarea polițienească internațională subdiviziunea specializată în cooperare polițienească internațională din subordinea Inspectoratului General al Poliției al Ministerului Afacerilor Interne. (5) Schimbul de informații se realizează în baza cererii de informații transmise de către autoritățile competente de aplicare a legii, prin intermediul punctului unic de contact, sau în mod direct, de către autoritățile competente, prin canalele de comunicare securizate avute la dispoziție. (6) Cerințele, și conținutul cererii de informații, procedurile operative, precum și termenele de soluționare a acestora se stabilesc prin hotărâre de Guvern.
(b) furnizarea de către un stat membru, din proprie inițiativă, a unor informații relevante punctelor de contact unice sau autorităților competente de aplicare a legii ale altor state membre, în special situațiile și modul în care trebuie furnizate aceste informații;	<i>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</i> Anexa nr.1 Punctul 10. PUC acționează ca interfață unică și centralizată între sistemele informaționale naționale și infrastructura centrală a Uniunii Europene, fiind structura administrativă și operațională desemnată la nivel național pentru a asigura fluxul informațional securizat cu statele	Compatibil	

	membre ale Uniunii Europene, alte state și organizațiile internaționale profilate pe schimbul de date și informații de natură infracțională, având următoarele atribuții funcționale și operaționale principale: 10.2. 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;		
(c) canalul implicit de comunicare care trebuie utilizat pentru toate schimburile de informații în temeiul prezentei directive și informațiile care trebuie furnizate punctelor de contact unice în legătură cu efectuarea de schimburi de informații direct între autoritățile competente de aplicare a legii;	<i>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</i> Anexa nr.1 Punctul 35. 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 S-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 de către PNC tehnic (STISC), în conformitate cu cerințele tehnice europene.	Compatibil	
(d) înființarea sau desemnarea și organizarea, sarcinile, componența și capacitățile punctelor de contact unice ale fiecărui stat membru, inclusiv privind implementarea și utilizarea unui sistem electronic unic de gestionare a cazurilor	<i>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</i> Anexa nr.1 Punctul 1. Scopul prezentului Regulament este intensificarea cooperării polițienești internaționale	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 6. Punctul unic de contact și atribuțiile acestuia (4) Subdiviziunea specializată în cooperare polițienească internațională

pentru îndeplinirea sarcinilor lor în temeiul prezentei directive.	pentru prevenirea, depistarea și investigarea infracțiunilor, precum și facilitarea căutării persoanelor dispărute și identificarea rămășițelor umane. Punctul 2. Scopul prezentului Regulament este intensificarea cooperării polițienești internaționale pentru prevenirea, depistarea și investigarea infracțiunilor, precum și facilitarea căutării persoanelor dispărute și identificarea rămășițelor umane. Punctul 3. PUC își desfășoară activitatea în conformitate cu Legea privind cooperarea polițienească internațională și tratatele internaționale la care Republica Moldova este parte. Punctul 9. Structura internă a PUC include următoarele subdiviziuni specializate ale DCPI: 9.1. <i>Secția Europol</i> – asigură schimbul de date și informații prin intermediul Router-ului și al sistemului EPRIS; 9.2. <i>Biroul Național Central Interpol</i> – asigură interfața cu baza de date SLTD privind documente de călătorie, vizele, titlurile de valoare, inclusiv a celor declarate false, furate sau pierdute, precum și a datelor privind permisele de conducere; 9.3. <i>Secția 24/7</i> – responsabilă de asigurarea fluxului informațional permanent și monitorizarea disponibilității sistemelor; 9.4. <i>Secția cooperare polițienească</i> – coordonează schimbul de date și informații în contextul evenimentelor majore cu dimensiune transfrontalieră; 9.5. <i>Biroul național SIRENE</i> – gestionează și coordonează alertele în cadrul Sistemului de Informații Schengen (SIS), asigurând schimbul de informații suplimentare legate de aceste alerte în conformitate cu procedurile prevăzute în Manualul SIRENE.	din cadrul Inspectoratului General al Poliției al Ministerului Afacerilor Interne cuprinde următoarele structuri, fără a se limita la acestea: 1) Biroul Național Central „INTERPOL”; 2) Punctul Național de Contact „EUROPOL”; 3) Biroul Național „SIRENE”; 4) Secția cooperare polițienească; 5) Secția 24/7 (suport operațional). Articolul 8. Sistemul de gestionare a cazurilor (1) În desfășurarea activităților specifice, subdiviziunea specializată în cooperare polițienească internațională a Inspectoratului General al Poliției utilizează Sistemul electronic de gestionare a cazurilor, care asigură cel puțin următoarele funcționalități: a) înregistrarea și trasabilitatea completă a cererilor de informații primite și transmise, a răspunsurilor aferente, a informațiilor furnizate din proprie inițiativă, precum și a refuzurilor motivate sau a solicitărilor de clarificări; b) înregistrarea comunicărilor, mesajelor primite și transmise; c) arhivarea electronică și jurnalizarea tuturor comunicărilor și mesajelor procesate prin canalele securizate;

	Punctul 15. Toate operațiunile de acces și schimb de date și informații sunt înregistrate în Sistemul electronic unic de gestionare a cazurilor, care asigură trasabilitatea acțiunilor de prelucrare și interoperabilitatea cu SIENA.		d) verificarea încrucișată automată (cross-checking) a interpelărilor cu datele existente în sistem, în scopul detectării suprapunerilor de informații solicitate și al valorificării informațiilor deținute; e) monitorizarea termenelor de răspuns, pentru a garanta furnizarea completă și rapidă a informațiilor în limitele legale stabilite; f) interoperabilitatea tehnică cu canalele securizate internaționale, permițând înregistrarea directă a fluxurilor de date în sistemul de gestionare a cazurilor; g) generarea rapoartelor statistice privind volumul și calitatea schimburilor de informații, în scopul evaluării și monitorizării; h) securitatea și auditarea accesului, prin înregistrarea strictă a oricărei activități de prelucrare a datelor, asigurând răspunderea personală a utilizatorilor; i) automatizarea fluxurilor de lucru și a procedurilor administrative interne. (2) Subdiviziunea specializată în cooperare polițienească internațională din cadrul Inspectoratului General al Poliției colectează, completează, stochează, prelucrează și examinează date în sistemul prevăzut la alin. (1) și realizează schimbul de informații potrivit atribuțiilor prevăzute de lege.

(2) Prezenta directivă nu se aplică schimburilor de informații între autoritățile competente de aplicare a legii care au scopul de a preveni, de a depista sau de a investiga infracțiunile reglementate în mod specific de alte acte legislative ale Uniunii. Fără a aduce atingere obligațiilor care le revin în temeiul prezentei directive sau al altor acte legislative ale Uniunii, statele membre pot adopta sau menține dispoziții care să faciliteze suplimentar schimbul de informații cu autoritățile competente de aplicare a legii din alte state membre în scopul prevenirii, depistării sau investigării infracțiunilor, inclusiv prin intermediul unor acorduri bilaterale sau multilaterale.	<i>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</i> Anexa nr.1 Punctul 3. PUC își desfășoară activitatea în conformitate cu Legea privind cooperarea polițienească internațională și tratatele internaționale la care Republica Moldova este parte. Punctul 4. În scopul transpunerii Directivei (UE) 2023/977, funcțiile de punct unic de contact pentru cooperarea polițienească internațională (<i>Single Point of Contact, în continuare – SPOC</i>) sunt exercitate de către PUC.	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 2. Scopul legii și domeniul de aplicare (3) Prevederile prezentei legi se aplică următoarelor forme de cooperare polițienească internațională: a) schimbul de informații polițienești, realizat pe cale bilaterală sau multilaterală, inclusiv prin intermediul canalelor securizate și a platformelor internaționale de cooperare, precum Interpol sau Europol; Prevederea stabilește o regulă de delimitare raportată la normele speciale (<i>lex specialis</i>) și o clauză de flexibilitate privind cooperarea aprofundată. Compatibilitatea este asigurată prin coroborare cu pct. 3 din prezentul proiect, care stipulează că PUC își desfășoară activitatea în conformitate cu tratatele internaționale la care Republica Moldova este parte. Pe de o parte, proiectul nu creează suprapuneri procedurale, schimburile de informații guvernate de reguli specifice păstrându-și regimul juridic propriu. Pe de altă parte, textul acordă statelor o facultate; proiectul de HG nu

			îngrădește și nu afectează aplicarea sau încheierea de către Republica Moldova a altor acorduri bilaterale ori multilaterale de cooperare polițienească (ex: cu statele vecine) care facilitează suplimentar schimbul de date prin termene sau proceduri mai rapide, respectând standardele minime instituite.
(3) Prezenta directivă nu le impune statelor membre nicio obligație: (a) de a obține informații prin intermediul unor măsuri coercitive;	<i>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</i> Anexa nr.1 Punctul 5. Prezentului Regulament, i se aplică noțiunile din Legea privind cooperarea polițienească internațională, precum și noțiunile utilizate cu următoarele semnificații: 5.9. <i>informații direct accesibile</i> – acele informații pe care personalul SPOC 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 SIS); 5.10. <i>informații indirect accesibile</i> – orice autoritate competentă de aplicare a legii, în sensul Legii privind cooperarea polițienească internațională, 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;	Compatibil	
(b) de a stoca informații exclusiv în scopul furnizării acestora autorităților competente de aplicare a legii din alte state membre;	<i>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</i>	Compatibil	

	Anexa nr.2 Punctul 2. Punctele Naționale de Contact (<i>în continuare – PNC</i>) sunt autoritățile competente responsabile de gestionarea tehnică și administrarea schimbului pentru o categorie specifică de date. Punctul 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.		
(c) de a furniza informații autorităților competente de aplicare a legii ale altor state membre pentru a fi utilizate ca mijloace de probă în procedurile judiciare.	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 Anexa nr.1 Punctul 33. Informațiile furnizate prin PUC nu pot fi utilizate ca mijloace de probă în procedurile judiciare fără acordul prealabil al statului care le-a furnizat.	Compatibil	Proiectul de lege privind cooperarea polițienească internațională Articolul 43. Protecția și scopul prelucrărilor datelor cu caracter personal (9) Datele cu caracter personal primite în temeiul prezentei legi nu pot fi transmise sau puse la dispoziția altor autorități ori entități, decât cu autorizarea prealabilă a autorității competente furnizoare și cu respectarea legislației naționale a acestei autorități, cu condiția ca o astfel de transmitere să fie permisă și de cadrul normativ aplicabil autorității furnizoare.

			Articolul 47. Transferul de date cu caracter personal către țări terțe și organizații internaționale (1) Autoritatea competentă poate transfera prin intermediul punctului unic de contact date cu caracter personal obținute în temeiul prezentei legi către un stat terț sau o organizație internațională, numai în condițiile prevăzute de legislația națională privind protecția datelor cu caracter personal și de actele normative aplicabile cooperării polițienești internaționale, cu autorizarea prealabilă a statului participant care a furnizat datele respective, cu condiția existenței unei decizii sau a unor garanții care asigură un nivel de protecție echivalent cu standardele europene aplicabile prelucrărilor efectuate de autorități competente. (2) În cazul în care datele furnizate de autoritățile competente ale Republicii Moldova sunt prelucrate ulterior de Europol, autorizarea pentru transferul acestora către un stat terț sau o organizație internațională se acordă de autoritatea competentă națională. (3) Prelucrarea datelor cu caracter personal în cadrul mecanismului prevăzut de prezenta lege se efectuează cu respectarea cadrului normativ privind protecția datelor cu caracter personal, în măsura în care prezenta lege nu prevede dispoziții speciale.

(4) Prezenta directivă nu instituie niciun drept de a utiliza informațiile furnizate în conformitate cu dispozițiile sale ca mijloace de probă în cadrul procedurilor judiciare. Statul membru care furnizează informațiile își poate da acordul ca acestea să fie utilizate ca mijloace de probă în cadrul procedurilor judiciare.	<i>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</i> Anexa nr.1 Punctul 33. Informațiile furnizate prin PUC nu pot fi utilizate ca mijloace de probă în procedurile judiciare fără acordul prealabil al statului care le-a furnizat.	Compatibil	
Articolul 2. Definiții În sensul prezentei directive: 1. „autoritate competentă de aplicare a legii” înseamnă orice autoritate polițienească, vamală sau altă autoritate a statelor membre competentă, în temeiul dreptului intern, să exercite autoritate și să ia măsuri coercitive în scopul prevenirii, depistării sau investigării infracțiunilor sau orice autoritate care participă la entități comune înființate între două sau mai multe state membre în scopul prevenirii, depistării sau investigării infracțiunilor, dar exclude agențiile sau unitățile a căror activitate include în special aspecte de securitate națională și ofițerii de legătură detașați în temeiul articolului 47 din Convenția de punere în aplicare a Acordului Schengen;		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 3. Noțiuni principale (2) În sensul prezentei legi, termenii și expresiile de mai jos au următoarele semnificații: 2) <i>autoritate competentă de aplicare a legii</i> – autoritate polițienească, judiciară, vamală sau altă autoritate de aplicare a legii, din Republica Moldova sau din alte țări, cu atribuții în prevenirea, depistarea sau investigarea infracțiunilor;
2. „autoritate de aplicare a legii desemnată” înseamnă o autoritate competentă de aplicare a legii care este autorizată să transmită cereri de informații punctelor de contact unice ale altor state membre în conformitate cu articolul 4 alineatul (1);	<i>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</i> Anexa nr.1 Punctul 5. Prezentei Regulament, i se aplică noțiunile din Legea privind cooperarea polițienească internațională, precum și noțiunile utilizate cu următoarele semnificații:	Compatibil	

	5.1. <i>autoritate de aplicare a legii desemnată</i> – orice autoritate competentă de aplicare a legii, în sensul Legii privind cooperarea polițienească internațională, 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;		
3. „infracțiune gravă” înseamnă oricare dintre următoarele: (a) o infracțiune astfel cum este menționată la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI a Consiliului ; (b) o infracțiune astfel cum este menționată la articolul 3 alineatul (1) sau (2) din Regulamentul (UE) 2016/794;		Compatibil	<i>Codul Penal al Republicii Moldova nr. 985/2002</i> Articolul 16. Clasificarea infracțiunilor (4) Infracțiuni grave se consideră faptele pentru care legea penală prevede pedeapsa maximă cu închisoare pe un termen de până la 12 ani inclusiv.
4. „informații” înseamnă orice conținut referitor la una sau mai multe persoane fizice sau juridice, fapte sau circumstanțe relevante pentru autoritățile competente de aplicare a legii în scopul îndeplinirii sarcinilor care le revin în temeiul dreptului intern de prevenire, depistare sau investigare a infracțiunilor, inclusiv informații operative în materie penală;		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 3. Noțiuni principale (2) În sensul prezentei legi, termenii și expresiile de mai jos au următoarele semnificații: 2) <i>informații</i> - orice conținut, documente, evidențe, activități sau rapoarte, indiferent de suport, formă, mod de exprimare sau de punere în circulație, referitoare la una sau mai multe persoane fizice sau juridice, fapte sau circumstanțe relevante pentru autoritățile competente în scopul îndeplinirii atribuțiilor care le revin în domeniul prevenirii, depistării sau investigării

			infrațiunilor, inclusiv informații operaționale în materie penală;
5. „informații disponibile” înseamnă informații direct accesibile și informații indirect accesibile;	<i>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</i> Anexa nr.1 Punctul 5. Prezentei Regulament, i se aplică noțiunile din Legea privind cooperarea polițienească internațională, precum și noțiunile utilizate cu următoarele semnificații: 5.9. <i>informații disponibile</i> – informații direct accesibile și informații indirect accesibile;	Compatibil	
6. „informații direct accesibile” înseamnă informații păstrate într-o bază de date care pot fi accesate direct de către punctul de contact unic sau de către o autoritate competentă de aplicare a legii din statul membru căruia i se solicită informațiile;	<i>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</i> Anexa nr.1 Punctul 5. Prezentei Regulament, i se aplică noțiunile din Legea privind cooperarea polițienească internațională, precum și noțiunile utilizate cu următoarele semnificații: 5.10. <i>informații direct accesibile</i> – acele informații pe care personalul SPOC 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 SIS);	Compatibil	
7. „informații indirect accesibile” înseamnă informații pe care un punct de contact unic sau o autoritate competentă de aplicare a legii din statul membru căruia i se solicită informațiile le poate obține de la alte autorități publice sau de la părți private stabilite în statul membru respectiv, în cazul în care acest lucru este	<i>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</i> Anexa nr.1 Punctul 5. Prezentei Regulament, i se aplică noțiunile din Legea privind cooperarea polițienească internațională, precum și noțiunile utilizate cu următoarele semnificații:	Compatibil	

permis de dreptul intern și în conformitate cu aceasta, fără măsuri coercitive;	5.11. <i>informații indirect accesibile</i> – datele care nu se află în sistemele interconectate ale SPOC și necesită o solicitare către alte autorități publice (ex: fisc, vamă) sau sectorul privat (ex: furnizori de servicii), fără dispunerea aplicării măsurilor coercitive, conform dreptului național;		
8. „date cu caracter personal” înseamnă datele cu caracter personal în sensul definiției de la articolul 3 punctul 1 din Directiva (UE) 2016/680.		Compatibil	<i>Legea nr. 195/2024 privind protecția datelor cu caracter personal</i> Articolul 4. Noțiuni <i>date cu caracter personal</i> – orice informații privind o persoană fizică identificată sau identificabilă (în continuare – persoană vizată). Persoana fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special, prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul ori mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale
Articolul 3. Principii referitoare la schimbul de informații În legătură cu toate schimburile de informații efectuate în temeiul prezentei directive, statele membre se asigură că: (a) informațiile disponibile pot fi furnizate punctului de contact unic sau autorităților competente de aplicare a legii ale altor state membre (denumit în continuare „principiul disponibilității”);		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 4. Principiile schimbului de informații (1) Schimbul de informații și cooperarea polițienească transfrontalieră realizate în temeiul prezentei legi, în vederea atingerii scopului și în limitele domeniului de aplicare al acesteia, se desfășoară cu respectarea următoarelor principii:

			c) <i>principiul disponibilității</i> – informațiile disponibile autorităților competente ale Republicii Moldova sunt puse la dispoziția autorităților competente solicitante ale altor state, în condițiile prezentei legi;
(b) condițiile pentru solicitarea de informații și furnizarea de informații punctelor de contact unice și autorităților competente de aplicare a legii ale altor state membre sunt echivalente cu cele aplicabile solicitării și furnizării unor informații similare în statul membru respectiv (denumit în continuare „principiul accesului echivalent”);		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 4. Principiile schimbului de informații (1) Schimbul de informații și cooperarea polițienească transfrontalieră realizate în temeiul prezentei legi, în vederea atingerii scopului și în limitele domeniului de aplicare al acesteia, se desfășoară cu respectarea următoarelor principii: b) <i>principiul accesului echivalent</i> – condițiile de solicitare și furnizare a informațiilor de către punctul național de contact și autoritățile competente sunt echivalente cu cele aplicabile solicitării și furnizării unor informații similare în statul solicitant, în măsura în care prezenta lege și acordurile internaționale aplicabile nu prevăd altfel;
(c) protejează informațiile furnizate punctului său de contact unic sau autorităților sale competente de aplicare a legii care sunt marcate ca fiind confidențiale în conformitate cu cerințele prevăzute în dreptul său intern, oferind un nivel de confidențialitate similar cu dreptul intern al statului membru care a		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 4. Principiile schimbului de informații (1) Schimbul de informații și cooperarea polițienească transfrontalieră realizate în temeiul

furnizat informațiile (denumit în continuare „principiul confidențialității”);			prezentei legi, în vederea atingerii scopului și în limitele domeniului de aplicare al acesteia, se desfășoară cu respectarea următoarelor principii: d) <i>principiul confidențialității</i> – autoritățile competente de aplicare a legii ale Republicii Moldova respectă confidențialitatea informațiilor primite de la autoritățile competente ale altor state, asigurând un nivel de protecție cel puțin echivalent cu cel aplicabil potrivit dreptului național și condițiilor comunicate de statul furnizor;
(d) în cazul în care informațiile solicitate au fost obținute inițial de la un alt stat membru sau de la o țară terță, furnizează astfel de informații unui alt stat membru sau Europol numai cu acordul statului membru sau al țării terțe care a furnizat inițial informațiile și în conformitate cu condițiile impuse de statul membru sau de țara terță care le-a furnizat inițial (denumit în continuare „principiul proprietății datelor”);		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 4. Principiile schimbului de informații (1) Schimbul de informații și cooperarea polițienească transfrontalieră realizate în temeiul prezentei legi, în vederea atingerii scopului și în limitele domeniului de aplicare al acesteia, se desfășoară cu respectarea următoarelor principii: e) <i>principiul proprietății și al controlului asupra difuzării ulterioare a datelor</i> – informațiile obținute de la un stat partener (sau de la un stat terț/organism internațional) pot fi transmise ulterior către o altă autoritate ori către un alt stat/organism internațional numai cu acordul prealabil al furnizorului inițial și cu respectarea condițiilor impuse de acesta, cu excepția

			cazurilor prevăzute expres de acordurile internaționale aplicabile;
(e) datele cu caracter personal care fac obiectul schimbului în temeiul prezentei directive care se dovedesc a fi inexacte, incomplete sau nu mai sunt actualizate, sunt șterse sau rectificate sau că prelucrarea lor este restricționată, după caz, și că orice destinatar este notificat fără întârziere (denumit în continuare „principiul fiabilității datelor”).		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 4. Principiile schimbului de informații (1) Schimbul de informații și cooperarea polițienească transfrontalieră realizate în temeiul prezentei legi, în vederea atingerii scopului și în limitele domeniului de aplicare al acesteia, se desfășoară cu respectarea următoarelor principii: f) <i>principiul fiabilității, exactității și actualizării datelor</i> – datele cu caracter personal care sunt inexacte, incomplete ori neactualizate se rectifică sau se șterg ori, după caz, prelucrarea acestora se restricționează, iar destinatarul este informat fără întârziere; Articolul 48. Responsabilitatea și instruirea (5) Autoritățile competente desemnate potrivit prezentei legi, asigură: h) corectarea, actualizarea sau ștergerea, după caz, a datelor primite de la o autoritate parteneră, în termen de cel mult 48 de ore de la primirea notificării că datele transmise au fost inexacte, neactuale ori au fost transmise cu încălcarea legii, cu informarea fără întârziere a autorității care a furnizat datele;

Articolul 4. Cererile de informații transmise punctului de contact unic (1) Statele membre se asigură că cererile de informații transmise de către punctul lor de contact unic și, în cazul în care dreptul lor intern prevede acest lucru, de către autoritățile de aplicare a legii desemnate, către punctul de contact unic al unui alt stat membru, respectă cerințele prevăzute la alineatele (2)-(6). Statele membre transmit Comisiei o listă a autorităților lor de aplicare a legii desemnate. Statele membre informează Comisia în cazul în care există modificări ale listei respective. Comisia publică online listele, precum și orice actualizare a acestora. Statele membre se asigură că atunci când autoritățile lor de aplicare a legii desemnate transmit o cerere de informații punctului de contact unic al altui stat membru, acestea transmit simultan o copie a cererii respective punctului lor de contact unic.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 41. Notificări (7) Punctul unic de contact notifică oficial Comisia Europeană, Agenția eu-LISA și Europol identitatea și datele de legătură ale punctelor naționale de contact desemnate conform art. 6 și utilizează lista centralizată a punctelor naționale de contact, gestionată de Comisia Europeană, pentru coordonarea operativă a schimbului de date.
(2) Statele membre pot permite, de la caz la caz, autorităților lor de aplicare a legii desemnate să nu transmită o copie a unei cereri de informații punctului lor de contact unic simultan cu transmiterea acesteia către punctul de contact unic al unui alt stat membru în conformitate cu alineatul (1), în cazul în care aceasta ar periclita una sau mai multe dintre următoarele: (a) o investigație extrem de sensibilă în curs pentru care prelucrarea informațiilor	<i>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</i> Anexa nr.1 Punctul 19. 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, 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	Compatibil	

necesită un nivel adecvat de confidențialitate;	celuilalt stat membru al Uniunii Europene sau alt stat. Punctul 20. Prin derogare de la pct. 19, 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: 20.1. o investigație extrem de sensibilă în curs, pentru care prelucrarea informațiilor necesită un nivel adecvat de confidențialitate; 20.2. un caz de terorism care nu implică situații de urgență sau de gestionare a crizelor; 20.3. siguranța unei persoane.		
(b) cazurile de terorism care nu implică situații de urgență sau de gestionare a crizelor;	<i>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</i> Anexa nr.1 Punctul 19. 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, 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. Punctul 20. Prin derogare de la pct. 19, 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: 20.1. o investigație extrem de sensibilă în curs, pentru care prelucrarea informațiilor necesită un nivel adecvat de confidențialitate;	Compatibil	

	20.2. un caz de terorism care nu implică situații de urgență sau de gestionare a crizelor; 20.3. siguranța unei persoane.		
(c) siguranța unei persoane;	<i>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</i> Anexa nr.1 Punctul 19. 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, 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 celui alt stat membru al Uniunii Europene sau alt stat. Punctul 20. Prin derogare de la pct. 19, 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: 20.1. o investigație extrem de sensibilă în curs, pentru care prelucrarea informațiilor necesită un nivel adecvat de confidențialitate; 20.2. un caz de terorism care nu implică situații de urgență sau de gestionare a crizelor; 20.3. siguranța unei persoane.	Compatibil	
(3) Statele membre se asigură că cererile de informații se transmit punctului de contact unic al altui stat membru numai atunci când există motive obiective să se creadă că: (a) informațiile solicitate sunt necesare atingerii scopului menționat la	<i>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</i> Anexa nr.1 Punctul 16. PUC asigură faptul că orice cerere de informații transmisă către un alt stat membru al Uniunii Europene sau alte state, este necesară și	Compatibil	

articolul 1 alineatul (1) primul paragraf și proporționale cu acesta; și	proporțională cu scopul urmărit și că informațiile solicitate sunt disponibile în statul respectiv. Punctul 17. În conformitate cu cerințele de necesitate și proporționalitate, PUC se asigură că cererile de informații sunt transmise către alte state membre ale Uniunii Europene sau alte state, numai în cazul în care: 17.1. există motive obiective care justifică că informațiile solicitate sunt necesare și proporționale pentru prevenirea, depistarea sau investigarea infracțiunilor; 17.2. există motive obiective care justifică că informațiile sunt disponibile în statul membru solicitat; 17.3. 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.		
(b) informațiile solicitate sunt disponibile statului membru respectiv.	<i>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</i> Anexa nr.1 Punctul 16. PUC asigură faptul că orice cerere de informații transmisă către un 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. Punctul 17. În conformitate cu cerințele de necesitate și proporționalitate, PUC se asigură că cererile de informații sunt transmise către alte state membre ale Uniunii Europene sau alte state, numai în cazul în care: 17.1. există motive obiective care justifică că informațiile solicitate sunt necesare și proporționale	Compatibil	

	pentru prevenirea, depistarea sau investigarea infracțiunilor; 17.2. există motive obiective care justifică că informațiile sunt disponibile în statul membru solicitat; 17.3. 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.		
(4) Statele membre se asigură că orice cerere de informații transmisă punctului de contact unic al altui stat membru precizează dacă este urgentă, iar în caz afirmativ, motivează urgența. Astfel de cereri de informații sunt considerate urgente dacă, având în vedere toate faptele și circumstanțele relevante ale cazului respectiv, există motive obiective să se creadă că informațiile solicitate îndeplinesc una sau mai multe dintre următoarele condiții: (a) sunt esențiale pentru prevenirea unei amenințări imediate și grave la adresa siguranței publice a unui stat membru;	<i>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</i> Anexa nr.1 Punctul 22. PUC marchează cererea ca fiind urgentă în situația în care informațiile solicitate îndeplinesc una sau mai multe dintre următoarele condiții: 22.1. sunt esențiale pentru prevenirea unei amenințări imediate și grave la adresa siguranței statului/publice;	Compatibil	
(b) sunt necesare pentru prevenirea unei amenințări iminente la adresa vieții sau integrității fizice ale unei persoane;	<i>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</i> Anexa nr.1 Punctul 22. PUC marchează cererea ca fiind urgentă în situația în care informațiile solicitate îndeplinesc una sau mai multe dintre următoarele condiții: 22.2. sunt necesare pentru prevenirea unei amenințări directe și iminente la adresa vieții sau integrității fizice a unei persoane;	Compatibil	

(c) sunt necesare pentru adoptarea unei decizii care poate implica menținerea unor măsuri restrictive care echivalează cu privarea de libertate;	<i>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</i> Anexa nr.1 Punctul 22. PUC marchează cererea ca fiind urgentă în situația în care informațiile solicitate îndeplinesc una sau mai multe dintre următoarele condiții: 22.3. sunt necesare pentru adoptarea unei decizii care poate implica menținerea unor măsuri restrictive care echivalează cu privarea de libertate;	Compatibil	
(d) există un risc iminent să își piardă relevanța dacă nu sunt furnizate de urgență și sunt considerate importante pentru prevenirea, depistarea sau investigarea infracțiunilor.	<i>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</i> Anexa nr.1 Punctul 22. PUC marchează cererea ca fiind urgentă în situația în care informațiile solicitate îndeplinesc una sau mai multe dintre următoarele condiții: 22.4. există un risc iminent să își piardă relevanța, dacă nu sunt furnizate de urgență, și sunt considerate importante pentru prevenirea, depistarea sau investigarea infracțiunilor;	Compatibil	
(5) Statele membre se asigură că cererile de informații transmise punctului de contact unic al altui stat membru conține toate detaliile necesare pentru a permite prelucrarea lor adecvată și rapidă în conformitate cu prezenta directivă, inclusiv cel puțin următoarele: (a) o precizare a informațiilor solicitate, care să fie cât mai detaliată posibil în circumstanțele respective;	<i>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</i> Anexa nr.1 Punctul 18. Cererile de informații transmise de PUC trebuie să fie complet documentate și să conțină cel puțin următoarele elemente: 18.1. identificarea solicitantului: denumirea autorității solicitante, data și numărul de înregistrare al solicitării;	Compatibil	

	18.2. scopul și justificarea: descrierea detaliată a scopului cererii, a faptelor investigate și a modului de operare, cu indicarea infracțiunii vizate (pregătite sau comise); 18.3. obiectul cererii: precizarea detaliată a informațiilor solicitate și a legăturii de cauzalitate dintre scopul solicitării și persoana sau entitatea vizată; 18.4. datele de identificare: datele cu caracter personal ale persoanelor implicate, extrase conform actelor de identitate (nume, prenume, data nașterii, cetățenie, serie/număr act); 18.5. regimul de urgență: precizarea caracterului de urgență (dacă este cazul) și motivarea obiectivă a acestuia, indicând riscul iminent pentru viața persoanelor sau riscul pierderii relevanței probatorii; 18.6. localizarea datelor: motivele obiective pentru care se consideră că statul solicitat deține informațiile.		
(b) o descriere a scopului în care sunt solicitate informațiile, inclusiv o descriere a faptelor și indicarea infracțiunii la care se referă;	<i>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</i> Anexa nr.1 Punctul 18. Cererile de informații transmise de PUC trebuie să fie complet documentate și să conțină cel puțin următoarele elemente: 18.1. identificarea solicitantului: denumirea autorității solicitante, data și numărul de înregistrare al solicitării; 18.2. scopul și justificarea: descrierea detaliată a scopului cererii, a faptelor investigate și a modului de operare, cu indicarea infracțiunii vizate (pregătite sau comise); 18.3. obiectul cererii: precizarea detaliată a informațiilor solicitate și a legăturii de cauzalitate	Compatibil	

	dintre scopul solicitării și persoana sau entitatea vizată; 18.4. datele de identificare: datele cu caracter personal ale persoanelor implicate, extrase conform actelor de identitate (nume, prenume, data nașterii, cetățenie, serie/număr act); 18.5. regimul de urgență: precizarea caracterului de urgență (dacă este cazul) și motivarea obiectivă a acestuia, indicând riscul iminent pentru viața persoanelor sau riscul pierderii relevanței probatorii; 18.6. localizarea datelor: motivele obiective pentru care se consideră că statul solicitat deține informațiile.		
(c) motivele obiective pentru care se consideră că statul membru solicitat dispune de informațiile solicitate;	<i>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</i> Anexa nr.1 Punctul 18. Cererile de informații transmise de PUC trebuie să fie complet documentate și să conțină cel puțin următoarele elemente: 18.1. identificarea solicitantului: denumirea autorității solicitante, data și numărul de înregistrare al solicitării; 18.2. scopul și justificarea: descrierea detaliată a scopului cererii, a faptelor investigate și a modului de operare, cu indicarea infracțiunii vizate (pregătite sau comise); 18.3. obiectul cererii: precizarea detaliată a informațiilor solicitate și a legăturii de cauzalitate dintre scopul solicitării și persoana sau entitatea vizată; 18.4. datele de identificare: datele cu caracter personal ale persoanelor implicate, extrase conform actelor de identitate (nume, prenume, data nașterii, cetățenie, serie/număr act);	Compatibil	

	18.5. regimul de urgență: precizarea caracterului de urgență (dacă este cazul) și motivarea obiectivă a acestuia, indicând riscul iminent pentru viața persoanelor sau riscul pierderii relevanței probatorii; 18.6. localizarea datelor: motivele obiective pentru care se consideră că statul solicitat deține informațiile.		
(d) o explicație a legăturii dintre scopul solicitării informațiilor și orice persoană fizică sau juridică sau entitate la care se referă informațiile, după caz;	<i>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</i> Anexa nr.1 Punctul 18. Cererile de informații transmise de PUC trebuie să fie complet documentate și să conțină cel puțin următoarele elemente: 18.1. identificarea solicitantului: denumirea autorității solicitante, data și numărul de înregistrare al solicitării; 18.2. scopul și justificarea: descrierea detaliată a scopului cererii, a faptelor investigate și a modului de operare, cu indicarea infracțiunii vizate (pregătite sau comise); 18.3. obiectul cererii: precizarea detaliată a informațiilor solicitate și a legăturii de cauzalitate dintre scopul solicitării și persoana sau entitatea vizată; 18.4. datele de identificare: datele cu caracter personal ale persoanelor implicate, extrase conform actelor de identitate (nume, prenume, data nașterii, cetățenie, serie/număr act); 18.5. regimul de urgență: precizarea caracterului de urgență (dacă este cazul) și motivarea obiectivă a acestuia, indicând riscul iminent pentru viața persoanelor sau riscul pierderii relevanței probatorii;	Compatibil	

	18.6. localizarea datelor: motivele obiective pentru care se consideră că statul solicitat deține informațiile.		
(e) motivele pentru care cererea este considerată urgentă, dacă este cazul, în conformitate cu alineatul (4);	<i>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</i> Anexa nr.1 Punctul 18. Cererile de informații transmise de PUC trebuie să fie complet documentate și să conțină cel puțin următoarele elemente: 18.1. identificarea solicitantului: denumirea autorității solicitante, data și numărul de înregistrare al solicitării; 18.2. scopul și justificarea: descrierea detaliată a scopului cererii, a faptelor investigate și a modului de operare, cu indicarea infracțiunii vizate (pregătite sau comise); 18.3. obiectul cererii: precizarea detaliată a informațiilor solicitate și a legăturii de cauzalitate dintre scopul solicitării și persoana sau entitatea vizată; 18.4. datele de identificare: datele cu caracter personal ale persoanelor implicate, extrase conform actelor de identitate (nume, prenume, data nașterii, cetățenie, serie/număr act); 18.5. regimul de urgență: precizarea caracterului de urgență (dacă este cazul) și motivarea obiectivă a acestuia, indicând riscul iminent pentru viața persoanelor sau riscul pierderii relevanței probatorii; 18.6. localizarea datelor: motivele obiective pentru care se consideră că statul solicitat deține informațiile.	Compatibil	
(f) restricții privind utilizarea informațiilor cuprinse în cerere în alte	<i>Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de</i>	Compatibil	

scopuri decât cele pentru care au fost transmise.	<i>Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații</i> Anexa nr.1 Punctul 18. Cererile de informații transmise de PUC trebuie să fie complet documentate și să conțină cel puțin următoarele elemente: 18.1. identificarea solicitantului: denumirea autorității solicitante, data și numărul de înregistrare al solicitării; 18.2. scopul și justificarea: descrierea detaliată a scopului cererii, a faptelor investigate și a modului de operare, cu indicarea infracțiunii vizate (pregătite sau comise); 18.3. obiectul cererii: precizarea detaliată a informațiilor solicitate și a legăturii de cauzalitate dintre scopul solicitării și persoana sau entitatea vizată; 18.4. datele de identificare: datele cu caracter personal ale persoanelor implicate, extrase conform actelor de identitate (nume, prenume, data nașterii, cetățenie, serie/număr act); 18.5. regimul de urgență: precizarea caracterului de urgență (dacă este cazul) și motivarea obiectivă a acestuia, indicând riscul iminent pentru viața persoanelor sau riscul pierderii relevanței probatorii; 18.6. localizarea datelor: motivele obiective pentru care se consideră că statul solicitat deține informațiile.		
(6) Statele membre se asigură că cererile de informații se transmit punctului de contact unic al altui stat membru într-una dintre limbile incluse în lista stabilită de celălalt stat membru în conformitate cu articolul 11.	<i>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</i> Anexa nr.1 Punctul 39. Schimbul de informații prin intermediul PUC se realizează în limba română în comunicarea cu autoritățile naționale și în limba	Compatibil	

	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.		
Articolul 5. Furnizarea de informații în baza cererilor transmise punctelor de contact unice (1) Statele membre se asigură că punctul lor de contact unic furnizează informațiile solicitate în conformitate cu articolul 4 cât mai curând posibil și, în orice caz, în următoarele termene, după caz: (a) opt ore în cazul cererilor urgente referitoare la informații direct accesibile;	<i>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</i> Anexa nr.1 Punctul 23. PUC furnizează informațiile solicitate în următoarele termene maxime: 23.1. 8 ore pentru cereri urgente referitoare la informații direct accesibile;	Compatibil	
(b) trei zile calendaristice în cazul cererilor urgente referitoare la informații indirect accesibile;	<i>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</i> Anexa nr.1 Punctul 23. PUC furnizează informațiile solicitate în următoarele termene maxime: 23.2. 3 zile calendaristice pentru cereri urgente referitoare la informații indirect accesibile;	Compatibil	
(c) șapte zile calendaristice, în cazul oricăror alte cereri. Termenele prevăzute la primul paragraf încep să curgă de la primirea cererii de informații.	<i>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</i> Anexa nr.1 Punctul 23. PUC furnizează informațiile solicitate în următoarele termene maxime: 23.3. 7 zile calendaristice pentru toate celelalte cereri.	Compatibil	
(2) Atunci când, în temeiul dreptului său intern, în conformitate cu articolul 9, un stat membru poate furniza informațiile	<i>Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de</i>	Compatibil	

solicitate numai după obținerea unei autorizații judiciare, respectivul stat membru se poate abate de la termenele stabilite la alineatul (1) de la prezentul articol în măsura în care acest lucru este necesar în scopul obținerii unei astfel de autorizații. În astfel de cazuri, statele membre se asigură că punctul lor de contact unic îndeplinește cumulativ următoarele sarcini: (a) informează imediat punctul de contact unic sau, după caz, autoritatea de aplicare a legii desemnată din statul membru solicitant cu privire la întârzierea preconizată, precizând durata estimată a întârzierii și motivele care stau la baza acesteia;	<i>Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații</i> Anexa nr.1 Punctul 26. În cazul în care legislația națională impune o autorizație judiciară pentru furnizarea informațiilor, PUC poate deroga de la termenele prevăzute la pct. 23, cu respectarea următoarelor condiții: 26.4. PUC informează imediat autoritatea solicitantă despre întârzierea preconizată, precizând motivele și durata estimată a acesteia;		
(b) ulterior menține informat punctul de contact unic sau, după caz, autoritatea de aplicare a legii desemnată din statul membru solicitant și furnizează informațiile solicitate cât mai curând posibil după obținerea autorizației judiciare.	<i>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</i> Anexa nr.1 Punctul 26. În cazul în care legislația națională impune o autorizație judiciară pentru furnizarea informațiilor, PUC poate deroga de la termenele prevăzute la pct. 23, cu respectarea următoarelor condiții: 26.5. pe parcursul procedurii, PUC menține informată autoritatea solicitantă și furnizează informațiile imediat după obținerea autorizației judiciare;	Compatibil	
(3) Statele membre se asigură că punctul lor de contact unic furnizează informațiile solicitate în conformitate cu articolul 4 punctului de contact unic sau, după caz, autorității de aplicare a legii desemnate din statul membru solicitant în	<i>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</i> Anexa nr.1	Compatibil	

limba în care a fost transmisă cererea de informații în conformitate cu articolul 4 alineatul (6). Statele membre se asigură că punctul lor de contact unic transmite o copie a informațiilor solicitate către punctul de contact unic al statului membru solicitant simultan cu furnizarea informațiilor solicitate către autoritatea de aplicare a legii desemnate a statului membru respectiv. Statele membre pot permite punctului lor de contact unic să nu transmită, simultan cu furnizarea de informații autorităților de aplicare a legii desemnate dintr-un alt stat membru în conformitate cu prezentul articol, o copie a informațiilor respective către punctul de contact unic al acelui alt stat membru, în cazul în care acest lucru ar periclita una sau mai multe dintre următoarele: (a) o investigație extrem de sensibilă în curs pentru care prelucrarea informațiilor necesită un nivel adecvat de confidențialitate; (b) cazurile de terorism care nu implică situații de urgență sau de gestionare a crizelor; (c) siguranța unei persoane.	Punctul 39. 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. Punctul 19. 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, 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. Punctul 20. Prin derogare de la pct. 19, 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: 20.1. o investigație extrem de sensibilă în curs, pentru care prelucrarea informațiilor necesită un nivel adecvat de confidențialitate; 20.2. un caz de terorism care nu implică situații de urgență sau de gestionare a crizelor; 20.3. siguranța unei persoane.		
Articolul 6. Refuzul de a da curs cererilor de informații (1) Statele membre se asigură că punctul lor de contact unic refuză să furnizeze informațiile solicitate în conformitate cu articolul 4 numai atunci când este aplicabil unul dintre următoarele motive:	<i>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</i> Anexa nr.1 Punctul 27. PUC poate refuza furnizarea informațiilor dacă este aplicabil unul dintre următoarele motive:	Compatibil	

(a) informațiile solicitate nu sunt disponibile punctului de contact unic și autorităților competente de aplicare a legii din statul membru solicitat;	<i>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</i> Anexa nr.1 Punctul 27. PUC poate refuza furnizarea informațiilor dacă este aplicabil unul dintre următoarele motive: 27.1. informațiile nu sunt disponibile sau cererea nu îndeplinește cerințele de necesitate și proporționalitate, prevăzute la pct. 17 din prezentul Regulament;	Compatibil	
(b) cererea de informații nu îndeplinește cerințele prevăzute la articolul 4;	<i>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</i> Anexa nr.1 Punctul 27. PUC poate refuza furnizarea informațiilor dacă este aplicabil unul dintre următoarele motive: 27.1. informațiile nu sunt disponibile sau cererea nu îndeplinește cerințele de necesitate și proporționalitate, prevăzute la pct. 17 din prezentul Regulament;	Compatibil	
(c) a fost refuzată acordarea autorizației judiciare necesare în temeiul dreptului intern al statului membru solicitat, în conformitate cu articolul 9;	<i>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</i> Anexa nr.1 Punctul 27. PUC poate refuza furnizarea informațiilor dacă este aplicabil unul dintre următoarele motive: 27.2. autorizația judiciară necesară a fost refuzată;	Compatibil	
(d) informațiile solicitate constituie date cu caracter personal, altele decât cele care se încadrează în categoriile de date cu	<i>Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de</i>	Compatibil	

caracter personal menționate la articolul 10 litera (b);	<i>Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații</i> Anexa nr.1 Punctul 27. PUC poate refuza furnizarea informațiilor dacă este aplicabil unul dintre următoarele motive: 27.5. informațiile solicitate constituie date cu caracter personal care nu se încadrează în categoriile permise pentru schimbul internațional;		
(e) s-a constatat că informațiile solicitate sunt inexacte, incomplete sau nu mai sunt actualizate și nu pot fi furnizate în conformitate cu articolul 7 alineatul (2) din Directiva (UE) 2016/680;	<i>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</i> Anexa nr.1 Punctul 27. PUC poate refuza furnizarea informațiilor dacă este aplicabil unul dintre următoarele motive: 27.6. informațiile sunt inexacte, incomplete sau nu mai sunt actualizate;	Compatibil	
(f) există motive obiective pentru a considera că furnizarea informațiilor solicitate: (i) ar contraveni intereselor esențiale ale securității naționale a statului membru solicitat sau ar afecta interesele respective; (ii) ar periclita succesul unei investigații în curs privind o infracțiune sau siguranța unei persoane; (iii) ar prejudicia interesele importante protejate ale unei persoane juridice;	<i>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</i> Anexa nr.1 Punctul 27. PUC poate refuza furnizarea informațiilor dacă este aplicabil unul dintre următoarele motive: 27.3. furnizarea datelor ar periclita interesele esențiale ale securității naționale, buna desfășurare a unei investigații în curs sau siguranța unei persoane sau ar prejudicia interesele importante protejate ale unei persoane juridice;	Compatibil	
(g) cererea se referă la: (i) o infracțiune care se pedepsește cu o pedeapsă maximă cu închisoarea până la un an în temeiul dreptului statului membru solicitat; sau	<i>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</i> Anexa nr.1	Compatibil	

(ii) o chestiune care nu constituie o infracțiune în temeiul dreptului statului membru solicitat;	Punctul 27. PUC poate refuza furnizarea informațiilor dacă este aplicabil unul dintre următoarele motive: 27.4. cererea vizează o infracțiune pedepsită cu maximum un an de închisoare conform dreptului intern sau o faptă care nu constituie infracțiune;		
(h) informațiile solicitate au fost obținute inițial de la un alt stat membru sau de la o țară terță, iar statul membru respectiv sau țara terță respectivă nu și-a dat acordul pentru furnizarea informațiilor. Statele membre depun toate diligențele pentru a evalua dacă cererea de informații transmisă punctului lor de contact unic este în conformitate cu cerințele prevăzute la articolul 4, în special pentru a constata dacă există o încălcare vădită a drepturilor fundamentale. Orice refuz de a da curs unei cereri de informații afectează numai partea din informațiile solicitate la care se referă motivele prevăzute la primul paragraf și, după caz, nu aduce atingere obligației de a furniza celelalte părți ale informațiilor respective în conformitate cu prezenta directivă.	<i>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</i> Anexa nr.1 Punctul 27. PUC poate refuza furnizarea informațiilor dacă este aplicabil unul dintre următoarele motive: 27.7. informațiile provin de la un alt stat sau țară terță care nu și-a dat acordul pentru retransmiterea acestora; 27.8. există o încălcare vădită a drepturilor fundamentale ale omului.	Compatibil	
(2) Statele membre se asigură că punctul lor de contact unic informează punctul de contact unic sau, după caz, autoritatea de aplicare a legii desemnată din statul membru solicitant cu privire la refuzul de a da curs cererii de informații, precizând motivele acestuia, cu respectarea termenelor prevăzute la articolul 5 alineatul (1).	<i>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</i> Anexa nr.1 Punctul 29. 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:	Compatibil	

	29.1. notificarea imediată: PUC informează autoritatea solicitantă în termenele prevăzute la pct. 23 despre imposibilitatea furnizării, precizând clar motivele refuzului sau natura defecțiunii tehnice;		
(3) După caz, statele membre se asigură că punctul lor de contact unic solicită imediat punctului de contact unic sau, după caz, autorității de aplicare a legii desemnate din statul membru solicitant clarificările sau precizările necesare pentru a prelucra o cerere de informații, în absența căroră cererea ar trebui refuzată. Termenele prevăzute la articolul 5 alineatul (1) se suspendă din momentul în care punctul de contact unic sau, după caz, autoritatea de aplicare a legii desemnată din statul membru solicitant primește cererea de clarificări sau precizări până în momentul în care clarificările sau precizările solicitate sunt furnizate.	<i>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</i> Anexa nr.1 Punctul 30. 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 căroră cererea ar trebui refuzată. Punctul 31. Termenele de furnizare a informațiilor prevăzute la pct. 23 se suspendă din momentul în care autoritatea solicitantă primește cererea de clarificări, până în momentul în care clarificările solicitate sunt furnizate către PUC.	Compatibil	
(4) Refuzurile de a da curs cererilor de informații, motivele unor asemenea refuzuri, cererile de clarificări sau precizări și clarificările și precizările menționate la alineatul (3) de la prezentul articol, precum și orice alte comunicări referitoare la cererile de informații transmise punctului de contact unic al altui stat membru se transmit în limba în care a fost transmisă cererea în conformitate cu articolul 4 alineatul (6).	<i>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</i> Anexa nr.1 Punctul 39. 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.	Compatibil	
Articolul 7. Furnizarea de informații din proprie inițiativă (1) Statele membre pot furniza din proprie inițiativă, prin intermediul	<i>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</i>	Compatibil	

punctului lor de contact unic sau prin intermediul autorităților lor competente de aplicare a legii, informațiile disponibile punctelor de contact unice sau autorităților competente de aplicare a legii din alte state membre, atunci când există motive obiective să se considere că astfel de informații ar putea fi relevante pentru statele membre respective în scopul prevenirii, depistării sau investigării infracțiunilor.	Anexa nr.1 Punctul 10. PUC acționează ca interfață unică și centralizată între sistemele informaționale naționale și infrastructura centrală a Uniunii Europene, fiind structura administrativă și operațională desemnată la nivel național pentru a asigura fluxul informațional securizat cu statele membre ale Uniunii Europene, alte state și organizațiile internaționale profilate pe schimbul de date și informații de natură infracțională, având următoarele atribuții funcționale și operaționale principale: 10.2. 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;		
(2) Statele membre se asigură că punctul lor de contact unic sau autoritățile lor competente de aplicare a legii furnizează din proprie inițiativă informațiile disponibile punctelor de contact unice sau autorităților competente de aplicare a legii din alte state membre, atunci când există motive obiective să se considere că astfel de informații ar putea fi relevante pentru statele membre respective în scopul prevenirii, depistării sau investigării infracțiunilor grave. Cu toate acestea, nu există o astfel de obligație atunci când informațiilor respective le sunt aplicabil motivele menționate la articolul 6 alineatul (1) litera (c) sau (f).	<i>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</i> Anexa nr.1 Punctul 32. 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.	Compatibil	
(3) Statele membre se asigură că, atunci când punctul lor de contact unic sau	<i>Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de</i>	Compatibil	

autoritățile lor competente de aplicare a legii furnizează informații din proprie inițiativă punctului de contact unic al altui stat membru în conformitate cu alineatul (1) sau (2), fac acest lucru în una dintre limbile incluse în lista stabilită de statul membru respectiv în conformitate cu articolul 11. Statele membre se asigură că, atunci când punctul lor de contact unic furnizează informații din proprie inițiativă autorității competente de aplicare a legii a unui alt stat membru, acesta transmite, simultan, o copie a informațiilor respective punctului de contact unic al celui alt stat membru. Statele membre se asigură că, atunci când autoritățile lor competente de aplicare a legii furnizează informații din proprie inițiativă unui alt stat membru, acestea transmit, simultan, o copie a informațiilor respective punctului de contact unic din statul lor membru și, dacă este cazul, punctului de contact unic al respectivului stat membru în cauză.	<i>Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații</i> Anexa nr.1 Punctul 19. 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, 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 celui alt stat membru al Uniunii Europene sau alt stat. Punctul 39. 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.		
(4) Statele membre pot permite autorităților lor competente de aplicare a legii să nu transmită, simultan cu furnizarea de informații punctului de contact unic sau autorităților competente de aplicare a legii dintr-un alt stat membru în conformitate cu prezentul articol, o copie a informațiilor respective către punctul de contact unic din statul lor membru sau către punctul de contact unic al statului membru respectiv, în cazul în care acest lucru ar periclita una sau mai multe dintre următoarele:	<i>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</i> Anexa nr.1 Punctul 20. Prin derogare de la pct. 19, 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: 20.1. o investigație extrem de sensibilă în curs, pentru care prelucrarea informațiilor necesită un nivel adecvat de confidențialitate;	Compatibil	

(a) o investigație extrem de sensibilă în curs pentru care prelucrarea informațiilor necesită un nivel adecvat de confidențialitate; (b) cazurile de terorism care nu implică situații de urgență sau de gestionare a crizelor; (c) siguranța unei persoane.	20.2. un caz de terorism care nu implică situații de urgență sau de gestionare a crizelor; 20.3. siguranța unei persoane.		
Articolul 8. Schimbul de informații în urma cererilor transmise direct autorităților competente de aplicare a legii (1) Statele membre se asigură că, atunci când punctul lor de contact unic transmite o cerere de informații direct autorității competente de aplicare a legii a altui stat membru, acesta transmite, simultan, o copie a cererii respective punctului de contact unic al celui alt stat membru. Statele membre se asigură că, în cazul în care una dintre autoritățile lor competente de aplicare a legii furnizează informații în urma unor astfel de cereri, aceasta transmite, simultan, o copie a acestor informații punctului de contact unic din statul său membru.	<i>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</i> Anexa nr.1 Punctul 19. 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, 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 celui alt stat membru al Uniunii Europene sau alt stat.	Compatibil	
(2) Statele membre se asigură că, în cazul în care una dintre autoritățile lor competente de aplicare a legii transmit o cerere de informații sau furnizează informații în temeiul unei astfel de cereri direct unei autorități competente de aplicare a legii dintr-un alt stat membru, aceasta transmite, simultan, o copie a cererii respective sau a informațiilor respective punctului de contact unic din	<i>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</i> Anexa nr.1 Punctul 19. 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	Compatibil	

statul său membru, precum și punctului de contact unic al celuilalt stat membru.	stat, 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.		
(3) Statele membre pot permite punctului lor de contact unic sau autorităților lor competente de aplicare a legii să nu transmită copii ale cererilor de informații sau informațiile menționate la alineatul (1) sau (2) în cazul în care acest lucru ar periclita una sau mai multe dintre următoarele: (a) o investigație extrem de sensibilă în curs pentru care prelucrarea informațiilor necesită un nivel adecvat de confidențialitate; (b) cazurile de terorism care nu implică situații de urgență sau de gestionare a crizelor; (c) siguranța unei persoane.	<i>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</i> Anexa nr.1 Punctul 20. Prin derogare de la pct. 19, 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: 20.1. o investigație extrem de sensibilă în curs, pentru care prelucrarea informațiilor necesită un nivel adecvat de confidențialitate; 20.2. un caz de terorism care nu implică situații de urgență sau de gestionare a crizelor; 20.3. siguranța unei persoane.	Compatibil	
Articolul 9. Autorizația judiciară (1) Un stat membru nu solicită o autorizație judiciară pentru furnizarea de informații punctului de contact unic sau autorităților competente de aplicare a legii dintr-un alt stat membru în temeiul capitolului II sau III, atunci când dreptul său intern nu impune o astfel de autorizație judiciară pentru furnizarea de informații similare în statul membru respectiv.	<i>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</i> Anexa nr.1 Punctul 26. În cazul în care legislația națională impune o autorizație judiciară pentru furnizarea informațiilor, PUC poate deroga de la termenele prevăzute la pct. 23, cu respectarea următoarelor condiții: 26.1. nu se solicită autorizație judiciară pentru furnizarea de informații către un alt stat membru dacă dreptul intern nu impune o astfel de procedură pentru furnizarea de informații similare în context național;	Compatibil	

(2) Statele membre se asigură că, atunci când dreptul lor intern impune obligația obținerii unei autorizații judiciare pentru furnizarea de informații punctului de contact unic sau autorităților competente de aplicare a legii din alt stat membru în temeiul capitolului II sau III, punctul lor de contact unic sau autoritățile lor competente de aplicare a legii iau imediat toate măsurile necesare, în conformitate cu dreptul lor intern, pentru a obține o astfel de autorizație judiciară cât mai curând posibil.	<i>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</i> Anexa nr.1 Punctul 26. În cazul în care legislația națională impune o autorizație judiciară pentru furnizarea informațiilor, PUC poate deroga de la termenele prevăzute la pct. 23, cu respectarea următoarelor condiții: 26.2. PUC sau autoritățile de aplicare a legii desemnate iau imediat toate măsurile necesare, conform dreptului intern, pentru a obține autorizația judiciară în cel mai scurt timp posibil;	Compatibil	
(3) Cererile de autorizații judiciare menționate la alineatul (2) sunt evaluate și soluționate în conformitate cu dreptul intern al statului membru al autorității judiciare competente.	<i>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</i> Anexa nr.1 Punctul 26. În cazul în care legislația națională impune o autorizație judiciară pentru furnizarea informațiilor, PUC poate deroga de la termenele prevăzute la pct. 23, cu respectarea următoarelor condiții: 26.2. PUC sau autoritățile de aplicare a legii desemnate iau imediat toate măsurile necesare, conform dreptului intern, pentru a obține autorizația judiciară în cel mai scurt timp posibil;	Compatibil	
Articolul 10. Norme suplimentare privind informațiile care constituie date cu caracter personal Statele membre se asigură că, atunci când punctul lor de contact unic sau autoritățile lor competente de aplicare a legii furnizează informații în temeiul capitolului II sau III care constituie date cu caracter personal:	<i>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</i> Anexa nr.1 Punctul 40. În cadrul schimburilor de informații reglementate de prezentul capitol, PUC asigură respectarea următoarelor standarde de calitate și protecție a datelor:	Compatibil	

(a) datele cu caracter personal sunt exacte, complete și actualizate, în conformitate cu articolul 7 alineatul (2) din Directiva (UE) 2016/680;	40.1. datele cu caracter personal furnizate sunt exacte, complete și actualizate;		
(b) categoriile de date cu caracter personal furnizate pentru fiecare categorie de persoane vizate rămân limitate la cele enumerate în secțiunea B din anexa II la Regulamentul (UE) 2016/794 și sunt necesare pentru atingerea scopului cererii și proporționale cu acesta;	<i>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</i> Anexa nr.1 Punctul 40. În cadrul schimburilor de informații reglementate de prezentul capitol, PUC asigură respectarea următoarelor standarde de calitate și protecție a datelor: 40.2. categoriile de date furnizate sunt limitate strict la cele enumerate în secțiunea B din anexa II la Regulamentul (UE) 2016/794 privind Europol și sunt transmise doar dacă sunt necesare și proporționale cu scopul cererii;	Compatibil	
(c) punctul lor de contact unic sau autoritățile lor competente de aplicare a legii furnizează, de asemenea, simultan și în măsura în care este posibil, elementele necesare care să îi permită punctului de contact unic sau autorității competente de aplicare a legii din celălalt stat membru să evalueze gradul de acuratețe, exhaustivitate și fiabilitate al datelor cu caracter personal, precum și în ce măsură datele cu caracter personal sunt actualizate.	<i>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</i> Anexa nr.1 Punctul 40. În cadrul schimburilor de informații reglementate de prezentul capitol, PUC asigură respectarea următoarelor standarde de calitate și protecție a datelor: 40.3. 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.	Compatibil	
Articolul 11. Lista limbilor (1) Statele membre stabilesc și actualizează o listă cu una sau mai multe limbi în care punctul lor de contact unic	<i>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</i>	Compatibil	

poate face schimb de informații. Această listă trebuie să includă limba engleză.	Anexa nr.1 Punctul 39. 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.		
(2) Statele membre furnizează Comisiei lista menționată la alineatul (1), precum și orice eventuale actualizări a acesteia. Comisia publică online o compilație a acestor liste și o actualizează.	<i>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</i> Anexa nr.1 Punctul 10. PUC acționează ca interfață unică și centralizată între sistemele informaționale naționale și infrastructura centrală a Uniunii Europene, fiind structura administrativă și operațională desemnată la nivel național pentru a asigura fluxul informațional securizat cu statele membre ale Uniunii Europene, alte state și organizațiile internaționale profilate pe schimbul de date și informații de natură infracțională, având următoarele atribuții funcționale și operaționale principale: 10.1. asigurarea notificării oficiale către Secretariatul General al Consiliului Uniunii Europene și Comisiei Europene, în termen de cel mult o lună de la data desemnării, cu privire la desemnarea PUC și a Punctelor Naționale de Contact (în continuare – PNC) pe domenii de competență, precum și a listei limbilor stabilite pentru schimbul de informații conform pct. 39, inclusiv a oricăror modificări ulterioare ale acestora, în vederea publicării în Jurnalul Oficial al Uniunii Europene sau pe platformele online dedicate ale Comisiei;	Compatibil	

Articolul 12. Furnizarea de informații către Europol (1) Statele membre se asigură că, atunci când punctul lor de contact unic sau autoritățile lor competente de aplicare a legii transmit cereri de informații, furnizează informații în temeiul unor astfel cereri de informații sau furnizează informații din proprie inițiativă în temeiul capitolului II sau III din prezenta directivă, personalul punctului lor de contact unic sau autorităților lor de aplicare a legii competente evaluează, de asemenea, de la caz la caz și sub rezerva articolului 7 alineatul (7) din Regulamentul (UE) 2016/794, dacă este necesar să transmită o copie a cererii de informații sau a informațiilor furnizate către Europol, în măsura în care informațiile la care se referă comunicarea privesc infracțiuni care se încadrează în domeniul de aplicare al obiectivelor Europol prevăzute la articolul 3 din Regulamentul (UE) 2016/794.	<i>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</i> Anexa nr.1 Punctul 10. PUC acționează ca interfață unică și centralizată între sistemele informaționale naționale și infrastructura centrală a Uniunii Europene, fiind structura administrativă și operațională desemnată la nivel național pentru a asigura fluxul informațional securizat cu statele membre ale Uniunii Europene, alte state și organizațiile internaționale profilate pe schimbul de date și informații de natură infracțională, având următoarele atribuții funcționale și operaționale principale: 10.2. 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; Punctul 32. 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. Punctul 19. 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, 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	Compatibil	

	celuilalt stat membru al Uniunii Europene sau alt stat.		
(2) Statele membre se asigură că, în cazul în care o copie a unei cereri de informații sau o copie a informațiilor este transmisă către Europol în temeiul alineatului (1) de la prezentul articol, scopurile prelucrării informațiilor și orice posibile restricții privind prelucrarea respectivă în temeiul articolului 19 din Regulamentul (UE) 2016/794 sunt comunicate în mod corespunzător către Europol. Statele membre se asigură că informațiile obținute inițial de la un alt stat membru sau de la o țară terță sunt transmise către Europol în temeiul alineatului (1) de la prezentul articol numai în cazul în care statul membru sau țara terță în cauză și-a dat acordul	<i>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</i> Anexa nr.1 Punctul 41. În cazul în care o copie a unei cereri de informații sau a informațiilor furnizate este transmisă către Europol, PUC se asigură că scopurile prelucrării și orice restricții privind prelucrarea respectivă, conform standardelor prevăzute la pct. 40, sunt comunicate în mod corespunzător agenției. Punctul 42. 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.	Compatibil	
Articolul 13. Canal de comunicare securizat (1) Statele membre se asigură că punctul lor de contact unic sau autoritățile lor competente de aplicare a legii utilizează aplicația de rețea pentru schimbul securizat de informații (SIENA) a Europol pentru a transmite cereri de informații, pentru a furniza informații în urma unor astfel de cereri sau pentru a furniza informații din proprie inițiativă în temeiul capitolului II sau III sau al articolului 12.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 6. Punctul unic de contact și atribuțiile acestuia (3) Punctul unic de contact are următoarele atribuții: e) exercită rolul de punct de contact pentru operațiuni comune regionale și internaționale și coordonează schimbul de informații prin intermediul canalelor de comunicare securizate avute la dispoziție;
(2) Statele membre pot permite punctelor lor de contact unice sau autorităților lor competente de aplicare a legii să nu utilizeze SIENA pentru a	<i>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</i>	Compatibil	

transmite cereri de informații, pentru a furniza informații ca urmare a unor astfel de cereri sau pentru a furniza informații din proprie inițiativă în temeiul capitolului II sau III sau al articolului 12, în unul sau mai multe dintre următoarele cazuri: (a) schimbul de informații necesită implicarea țărilor terțe sau a organizațiilor internaționale sau există motive obiective pentru a considera că va fi necesară implicarea acestora într-o etapă ulterioară, inclusiv prin intermediul canalului de comunicare al Interpolului; (b) caracterul urgent al cererii de informații necesită utilizarea temporară a unui alt canal de comunicare; (c) un incident tehnic sau operațional neașteptat împiedică utilizarea SIENA pentru schimbul de informații de către punctelor lor de contact unice sau autorităților lor competente de aplicare a legii.	Anexa nr.1 Punctul 36. PUC este autoritatea responsabilă de decizia privind canalul de cooperare utilizat pentru schimbul de informații, având competența de a autoriza utilizarea altor canale securizate (Interpol, SELEC sau canale bilaterale) în funcție de disponibilitatea tehnică a partenerilor, cerințele de interoperabilitate și necesitatea asigurării eficienței schimbului, fără a afecta securitatea și integritatea datelor, luând în considerare următoarele situații și criterii: 36.1. necesitatea interoperabilității, în cazul în care statul membru partener sau țara terță nu utilizează canalul SIENA sau invocă lipsa acordurilor tehnice necesare; 36.2. implicarea unor țări terțe sau a organizațiilor internaționale care utilizează platforme de comunicare specifice (ex. Interpol, SELEC); 36.3. urgența majoră care impune utilizarea temporară a celui mai rapid canal disponibil pentru salvarea vieții sau integrității unei persoane; 36.4. existența unui incident tehnic neașteptat care împiedică utilizarea temporară a SIENA; 36.5. eficiența schimbului, atunci când natura datelor sau specificul canalului (ex: SELEC pentru criminalitatea organizată în regiune) garantează un rezultat operativ superior fără a afecta securitatea datelor.		
(3) Statele membre se asigură că punctul lor de contact unic, precum și toate autoritățile lor competente de aplicare a legii care ar putea fi implicate în schimbul de informații în temeiul prezentei directive sunt conectate direct la SIENA, inclusiv, după caz, prin dispozitive mobile.	<i>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</i> Anexa nr.1 Punctul 35. PUC, precum și toate PNC-urile care ar putea fi implicate în schimbul de informații, sunt conectate direct la aplicația securizată SIENA,	Compatibil	

	inclusiv, după caz, prin dispozitive mobile securizate. Schimbul de informații și comunicarea operațională se realizează prin intermediul rețelei securizate S-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 de către PNC tehnic (STISC), în conformitate cu cerințele tehnice europene.		
Articolul 14. Înființare sau desemnare, sarcini și capacități ale punctului de contact unic (1) Fiecare stat membru înființează sau desemnează un punct de contact unic. Punctul de contact unic este entitatea centrală responsabilă de coordonarea și facilitarea schimbului de informații în temeiul prezentei directive.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 6. Punctul unic de contact și atribuțiile acestuia (1) Se desemnează în calitate de punct unic de contact pentru cooperarea polițienească internațională subdiviziunea specializată în cooperare polițienească internațională din subordinea Inspectoratului General al Poliției al Ministerului Afacerilor Interne.
(2) Statele membre se asigură că punctul lor de contact unic este echipat și împuternicit să îndeplinească cel puțin toate sarcinile următoare: (a) primirea și analizarea cererilor de informații transmise în conformitate cu articolul 4 în limbile notificate în conformitate cu articolul 11 alineatul (2); (b) direcționarea cererilor de informații către autoritățile de aplicare a legii competente și relevante și, atunci când este necesar, coordonarea între acestea în ceea ce privește prelucrarea unor astfel de		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 6. Punctul unic de contact și atribuțiile acestuia (3) Punctul unic de contact are următoarele atribuții: a) recepționează, înregistrează, stabilește gradul de importanță, și examinează, conform competenței, cererile de informații adresate de către alte țări Republicii Moldova, precum și cele adresate altor țări de către

cereri și furnizarea de informații în urma unor asemenea cereri; (c) coordonarea analizării și structurării informațiilor în vederea furnizării acestora punctelor de contact unice și, după caz, autorităților competente de aplicare a legii ale altor state membre; (d) furnizarea, la cerere sau din proprie inițiativă, de informații altor state membre, în conformitate cu articolele 5 și 7; (e) refuzul de a furniza informații în conformitate cu articolul 6 și, atunci când este necesar, solicitarea de clarificări sau precizări în conformitate cu articolul 6 alineatul (3); f) transmiterea de cereri de informații punctelor de contact unice ale altor state membre în conformitate cu articolul 4 și, atunci când este necesar, furnizarea de clarificări sau precizări în conformitate cu articolul 6 alineatul (3).			autoritățile competente naționale, conform competenței; b) direcționează cererile de informații către autoritățile competente naționale în cazul indisponibilității datelor în sistemele informaționale la care deține acces direct, și la necesitate, coordonează între acestea procesarea cererilor și furnizarea informațiilor; d) furnizează, la solicitare sau din oficiu, informații de specialitate relevante către autoritățile competente naționale și internaționale, în sprijinul activităților de prevenire, investigare și combatere a infracțiunilor; e) exercită rolul de punct de contact pentru operațiuni comune regionale și internaționale și coordonează schimbul de informații prin intermediul canalelor de comunicare securizate avute la dispoziție;
(3) Statele membre se asigură că: (a) punctul lor de contact unic: (i) are acces la toate informațiile disponibile autorităților lor competente de aplicare a legii, în măsura în care acest lucru este necesar pentru îndeplinirea sarcinilor care îi revin în temeiul prezentei directive; (ii) își îndeplinește sarcinile 24 de ore din 24, 7 zile din 7; (iii) are la dispoziție personal calificat, instrumente operaționale adecvate, resurse tehnice și financiare, infrastructură	<i>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</i> Anexa nr.1 Punctul 6. PUC își desfășoară activitatea în conformitate cu următoarele principii generale stabilite pentru activitatea Poliției: 6.4. <i>controlul ierarhic permanent, răspunderea personală și profesionalismul</i> - deciziile nu sunt pur automatizate, orice rezultat este verificat manual de personal calificat, care poartă răspundere personală pentru validitatea datelor;	Compatibil	

și capacități necesare, inclusiv în materie de traducere, pentru a-și îndeplini sarcinile în mod adecvat, efectiv și rapid, în conformitate cu prezenta directivă, inclusiv, după caz, cu respectarea termenelor prevăzute la articolul 5 alineatul (1);	Punctul 10. PUC acționează ca interfață unică și centralizată între sistemele informaționale naționale și infrastructura centrală a Uniunii Europene, fiind structura administrativă și operațională desemnată la nivel național pentru a asigura fluxul informațional securizat cu statele membre ale Uniunii Europene, alte state și organizațiile internaționale profilate pe schimbul de date și informații de natură infracțională, având următoarele atribuții funcționale și operaționale principale: 10.9. asigurarea accesului efectiv al personalului desemnat pentru cooperarea cu Europol la toate bazele de date naționale relevante, în limitele competențelor legale, pentru a permite schimbul rapid de date și informații privind infracțiunile transfrontaliere, cu accent pe traficul ilicit de vehicule; Punctul 13. 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. Punctul 34. 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 riguroasă a legislației privind protecția datelor cu caracter personal și a normelor speciale privind securitatea informațiilor cu accesibilitate limitată. Punctul 23. PUC furnizează informațiile solicitate în următoarele termene maxime: 23.1. 8 ore pentru cereri urgente referitoare la informații direct accesibile;		

	23.2. 3 zile calendaristice pentru cereri urgente referitoare la informații indirect accesibile; 23.3. 7 zile calendaristice pentru toate celelalte cereri.		
(b) autoritățile judiciare competente să acorde autorizațiile judiciare necesare în temeiul dreptului intern în conformitate cu articolul 9 sunt la dispoziția punctului de contact unic, la cerere, 24 de ore din 24, 7 zile din 7.	<i>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</i> Anexa nr.1 Punctul 26. În cazul în care legislația națională impune o autorizație judiciară pentru furnizarea informațiilor, PUC poate deroga de la termenele prevăzute la pct. 23, cu respectarea următoarelor condiții: 26.2. PUC sau autoritățile de aplicare a legii desemnate iau imediat toate măsurile necesare, conform dreptului intern, pentru a obține autorizația judiciară în cel mai scurt timp posibil; 26.3. examinarea cererilor de autorizare judiciară se realizează prin mecanisme de permanență (24/7), astfel încât să fie garantată respectarea termenelor de urgență prevăzute de prezentul Regulament;	Compatibil	
(4) În termen de o lună de la înființarea sau desemnarea punctului lor de contact unic, statele membre notifică acest lucru Comisiei. Statele membre informează Comisia în cazul în care intervin modificări în ceea ce privește punctul lor de contact unic. Comisia publică respectivele notificări, precum și eventualele actualizări ale acestora în Jurnalul Oficial al Uniunii Europene.	<i>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</i> Anexa nr.1 Punctul 10. PUC acționează ca interfață unică și centralizată între sistemele informaționale naționale și infrastructura centrală a Uniunii Europene, fiind structura administrativă și operațională desemnată la nivel național pentru a asigura fluxul informațional securizat cu statele membre ale Uniunii Europene, alte state și organizațiile internaționale profilate pe schimbul de date și informații de natură infracțională, având	Compatibil	

	următoarele atribuții funcționale și operaționale principale: 10.1. asigurarea notificării oficiale către Secretariatul General al Consiliului Uniunii Europene și Comisiei Europene, în termen de cel mult o lună de la data desemnării, cu privire la desemnarea PUC și a Punctelor Naționale de Contact (în continuare – PNC) pe domenii de competență, precum și a listei limbilor stabilite pentru schimbul de informații conform pct. 39, inclusiv a oricăror modificări ulterioare ale acestora, în vederea publicării în Jurnalul Oficial al Uniunii Europene sau pe platformele online dedicate ale Comisiei;		
Articolul 15. Organizare, componență și formare (1) Statele membre stabilesc organizarea și componența punctului lor de contact unic astfel încât acesta să își poată îndeplini sarcinile care îi revin în temeiul prezentei directive în mod eficient și efectiv.	<i>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</i> Anexa nr.1 Punctul 4. În scopul transpunerii Directivei (UE) 2023/977, funcțiile de punct unic de contact pentru cooperarea polițienească internațională (Single Point of Contact, în continuare – SPOC) sunt exercitate de către PUC. Punctul 8. 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.	Compatibil	
(2) Statele membre se asigură că punctul lor de contact unic este compus din personal al autorităților lor competente de aplicare a legii a căror implicare este necesară pentru a asigura un schimb adecvat și rapid de informații în temeiul		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 6. Punctul unic de contact și atribuțiile acestuia

prezentei directive, inclusiv cel puțin următoarele, în măsura în care statul membru în cauză este obligat prin legislația relevantă sau prin acorduri internaționale să înființeze sau să desemneze astfel de unități sau birouri: (a) unitatea națională a Europol, instituită prin articolul 7 din Regulamentul (UE) 2016/794; (b) biroul SIRENE, instituit prin articolul 7 alineatul (2) din Regulamentul (UE) 2018/1862; (c) biroul central național al Interpol, instituit prin articolul 32 din Statutul Organizației Internaționale de Poliție Criminală – Interpol.			(4) Subdiviziunea specializată în cooperare polițienească internațională din cadrul Inspectoratului General al Poliției al Ministerului Afacerilor Interne cuprinde următoarele structuri, fără a se limita la acestea: 1) Biroul Național Central „INTERPOL”; 2) Punctul Național de Contact „EUROPOL”; 3) Biroul Național „SIRENE”; 4) Secția cooperare polițienească; 5) Secția 24/7 (suport operațional).
(3) Statele membre se asigură că personalul punctului lor de contact unic are calificările necesare pentru a-și îndeplini funcțiile în temeiul prezentei directive. În acest scop, statele membre oferă personalului din cadrul punctului lor de contact unic acces la formare adecvată și periodică, în special în ceea ce privește: (a) utilizarea instrumentelor de prelucrare a datelor utilizate în cadrul punctului de contact unic, în special SIENA și sistemul de gestionare a cazurilor; (b) aplicarea dreptului Uniunii relevant și a dreptului intern relevant pentru activitățile punctului de contact unic în temeiul prezentei directive, în special în ceea ce privește protecția datelor cu caracter personal, inclusiv Directiva (UE) 2016/680, în ceea ce privește cooperarea transfrontalieră între autoritățile de		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 48. Responsabilitatea și instruirea (3) Formarea prevăzută la alin. (2) include, în mod obligatoriu, instruirea privind: a) protecția datelor cu caracter personal și securitatea informației în cadrul schimbului de date realizat în temeiul prezentei legi; b) verificarea și confirmarea exactă a concordanțelor/rezultatelor obținute în urma căutărilor și comparațiilor efectuate, inclusiv prin proceduri de examinare manuală atunci când este cazul.

aplicare a legii, inclusiv prezenta directivă și Regulamentul (UE) 2016/794, și în ceea ce privește prelucrarea informațiilor confidențiale; (c) utilizarea limbilor incluse în lista stabilită de statul membru în cauză în temeiul articolului 11.			
Articolul 16. Sistemul de gestionare a cazurilor (1) Statele membre se asigură că punctul lor de contact unic implementează și utilizează un sistem electronic unic de gestionare a cazurilor ca registru care îi permite punctului de contact unic să își îndeplinească sarcinile care îi revin în temeiul prezentei directive. Sistemul de gestionare a cazurilor trebuie să aibă cel puțin toate funcțiile și capacitățile următoare: (a) înregistrarea cererilor de informații primite și transmise, astfel cum sunt menționate la articolele 5 și 8, precum și a oricăror alte comunicări cu punctele de contact unice și, după caz, cu autoritățile competente de aplicare a legii din alte state membre cu privire la astfel de cereri, inclusiv a informațiilor privind refuzurile de a da curs cererilor de informații și cererile și furnizarea de clarificări sau precizări astfel cum sunt menționate la articolul 6 alineatul (2) și, respectiv, alineatul (3);		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 8. Sistemul de gestionare a cazurilor (1) În desfășurarea activităților specifice, subdiviziunea specializată în cooperare polițienească internațională a Inspectoratului General al Poliției utilizează Sistemul electronic de gestionare a cazurilor, care asigură cel puțin următoarele funcționalități:
(b) înregistrarea comunicărilor dintre punctul de contact unic și autoritățile competente de aplicare a legii, în temeiul articolului 14 alineatul (2) litera (b);		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 8. Sistemul de gestionare a cazurilor

			(1) În desfășurarea activităților specifice, subdiviziunea specializată în cooperare polițienească internațională a Inspectoratului General al Poliției utilizează Sistemul electronic de gestionare a cazurilor, care asigură cel puțin următoarele funcționalități: a) înregistrarea și trasabilitatea completă a cererilor de informații primite și transmise, a răspunsurilor aferente, a informațiilor furnizate din proprie inițiativă, precum și a refuzurilor motivate sau a solicitărilor de clarificări;
(c) înregistrarea furnizărilor de informații punctului de contact unic și, după caz, autorităților competente de aplicare a legii din alte state membre, în conformitate cu articolele 5, 7 și 8;		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 8. Sistemul de gestionare a cazurilor (1) În desfășurarea activităților specifice, subdiviziunea specializată în cooperare polițienească internațională a Inspectoratului General al Poliției utilizează Sistemul electronic de gestionare a cazurilor, care asigură cel puțin următoarele funcționalități: b) înregistrarea comunicărilor, mesajelor primite și transmise; c) arhivarea electronică și jurnalizarea tuturor comunicărilor și mesajelor procesate prin canalele securizate;
(d) verificarea încrucișată a cererilor de informații primite menționate la articolele 5 și 8 cu informațiile disponibile punctului de contact unic, inclusiv cu informațiile furnizate în conformitate cu articolul 5		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 8. Sistemul de gestionare a cazurilor

alineatul (3) al doilea paragraf și cu articolul 7 alineatul (3) al doilea paragraf și cu alte informații relevante înregistrate în sistemul de gestionare a cazurilor;			(1) În desfășurarea activităților specifice, subdiviziunea specializată în cooperare polițienească internațională a Inspectoratului General al Poliției utilizează Sistemul electronic de gestionare a cazurilor, care asigură cel puțin următoarele funcționalități: d) verificarea încrucișată automată (cross-checking) a interpelărilor cu datele existente în sistem, în scopul detectării suprapunerilor de informații solicitate și al valorificării informațiilor deținute;
(e) asigurarea răspunsului adecvat și rapid la cererile de informații primite menționate la articolul 4, în special în vederea respectării termenelor pentru furnizarea informațiilor solicitate prevăzute la articolul 5;		Compatibil	Proiectul de lege privind cooperarea polițienească internațională Articolul 8. Sistemul de gestionare a cazurilor (1) În desfășurarea activităților specifice, subdiviziunea specializată în cooperare polițienească internațională a Inspectoratului General al Poliției utilizează Sistemul electronic de gestionare a cazurilor, care asigură cel puțin următoarele funcționalități: e) monitorizarea termenelor de răspuns, pentru a garanta furnizarea completă și rapidă a informațiilor în limitele legale stabilite;
(f) interoperabilitatea cu SIENA, asigurându-se, în special, că toate comunicările care sunt primite prin intermediul SIENA pot fi înregistrate direct în sistemul de gestionare a cazurilor și că toate comunicările care sunt transmise prin intermediul SIENA pot fi		Compatibil	Proiectul de lege privind cooperarea polițienească internațională Articolul 8. Sistemul de gestionare a cazurilor (1) În desfășurarea activităților specifice, subdiviziunea specializată în

transmise direct din sistemul de gestionare a cazurilor;			cooperare polițienească internațională a Inspectoratului General al Poliției utilizează Sistemul electronic de gestionare a cazurilor, care asigură cel puțin următoarele funcționalități: f) interoperabilitatea tehnică cu canalele securizate internaționale, permițând înregistrarea directă a fluxurilor de date în sistemul de gestionare a cazurilor;
(g) generarea de statistici privind schimburile de informații efectuate în temeiul prezentei directive în scopul evaluării și monitorizării, în special în sensul articolului 18;		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 8. Sistemul de gestionare a cazurilor (1) În desfășurarea activităților specifice, subdiviziunea specializată în cooperare polițienească internațională a Inspectoratului General al Poliției utilizează Sistemul electronic de gestionare a cazurilor, care asigură cel puțin următoarele funcționalități: g) generarea rapoartelor statistice privind volumul și calitatea schimburilor de informații, în scopul evaluării și monitorizării;
(h) înregistrarea accesului și a altor activități de prelucrare în legătură cu informațiile conținute în sistemul de gestionare a cazurilor, din motive de răspundere și securitate cibernetică, în conformitate cu articolul 25 din Directiva (UE) 2016/680.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 8. Sistemul de gestionare a cazurilor (1) În desfășurarea activităților specifice, subdiviziunea specializată în cooperare polițienească internațională a Inspectoratului General al Poliției utilizează Sistemul electronic de

			gestionare a cazurilor, care asigură cel puțin următoarele funcționalități: h) securitatea și auditarea accesului, prin înregistrarea strictă a oricărei activități de prelucrare a datelor, asigurând răspunderea personală a utilizatorilor; i) automatizarea fluxurilor de lucru și a procedurilor administrative interne.
(2) Statele membre se asigură că toate riscurile în materie de securitate cibernetică legate de sistemul de gestionare a cazurilor, în special în ceea ce privește arhitectura, guvernanta și controlul acestuia, sunt gestionate și abordate într-un mod prudent și eficace și că sunt prevăzute garanții adecvate împotriva accesului neautorizat și a abuzului.	<i>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</i> Anexa nr.1 Punctul 91. În scopul protejării infrastructurii tehnice, autoritatea competentă sau PNC implementează următoarele măsuri de securitate în cadrul sistemelor proprii: 91.1. protecția fizică a echipamentelor și instalațiilor de prelucrare a datelor; 91.2. împiedicarea accesului neautorizat la suporturile de date și echipamentele de prelucrare; 91.3. utilizarea mecanismelor de autentificare securizată (nume de utilizator individuale și coduri de acces) pentru personalul autorizat; 91.4. aplicarea tehnicilor de criptare corespunzătoare pentru transportul datelor către infrastructurile centrale; 91.5. asigurarea planurilor de redresare în caz de dezastru pentru restabilirea funcționării sistemelor. Punctul 92. 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.	Compatibil	

Anexa nr.2

Punctul 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.

Punctul 38. PNC-urile sunt responsabile de implementarea măsurilor de securitate pentru protejarea integrității și confidențialității datelor în timpul procesului de transmitere către PUC, prin:

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

38.2. *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;

38.3. *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.

Punctul 78. STISC este desemnat în calitate de PNC tehnic pentru rețeaua securizată S-TESTA, fiind responsabil de asigurarea conectivității, funcționării, disponibilității și securității canalului național de comunicații utilizat pentru schimbul de date.

Punctul 79. În exercitarea atribuțiilor sale, STISC îndeplinește următoarele funcții principale:

79.1. administrează suportul tehnic pentru conectarea și funcționarea Router-ului UE, a sistemului EPRIS și a sistemului EUCARIS,

	garantând transportul securizat al datelor pe segmentul național; 79.3. asigură conectivitatea tehnică și securitatea canalului național de comunicații necesar funcționării interfețelor de acces la Sistemul de Informații Schengen (SIS), în conformitate cu cerințele tehnice europene.		
(3) Statele membre se asigură că sistemul de gestionare a cazurilor conține date cu caracter personal numai atât timp cât este necesar și proporțional ca punctul de contact unic să îndeplinească sarcinile care îi sunt atribuite în temeiul prezentei directive și că datele cu caracter personal conținute în acesta sunt ulterior șterse în mod irevocabil.	<i>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</i> Anexa nr.1 Punctul 37. Toate operațiunile PUC sunt înregistrate într-un sistem electronic unic de gestionare a cazurilor, care trebuie să respecte următoarele reguli: 37.1. înregistrările (log-urile) sunt păstrate timp de 3 ani pentru monitorizarea legalității; 37.2. conține date cu caracter personal doar atât timp cât este necesar și proporțional pentru îndeplinirea sarcinilor; 37.3. asigură ștergerea irevocabilă a datelor care nu mai sunt necesare;	Compatibil	
(4) Statele membre se asigură că punctul lor de contact unic reexaminează respectarea alineatului (3) pentru prima dată în termen de cel mult șase luni de la încheierea schimbului de informații și, ulterior, în mod regulat.	<i>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</i> Anexa nr.1 Punctul 37. Toate operațiunile PUC sunt înregistrate într-un sistem electronic unic de gestionare a cazurilor, care trebuie să respecte următoarele reguli: 37.4. este supus unei reexaminări privind necesitatea păstrării datelor în termen de cel mult 6 luni de la încheierea schimbului de informații.	Compatibil	
Articolul 17. Cooperarea dintre punctele de contact unice	<i>Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de</i>	Compatibil	

(1) Statele membre încurajează cooperarea practică între punctele lor de contact unice și autoritățile competente de aplicare a legii în sensul prezentei directive.	<i>Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații</i> Anexa nr.1 Punctul 8. 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.		
(2) Statele membre se asigură că șefii punctelor de contact unice se reunesc cel puțin o dată pe an pentru a evalua calitatea cooperării dintre serviciile lor, pentru a discuta măsurile tehnice sau organizatorice necesare în caz de dificultăți și pentru a clarifica procedurile acolo unde este necesar.	<i>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</i> Anexa nr.1 Punctul 12. În scopul consolidării cooperării polițienești internaționale, conducătorul PUC are următoarele responsabilități de coordonare internațională: 12.1. 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; 12.2. evaluează, în cadrul acestor reuniuni, calitatea cooperării dintre serviciile naționale și cele străine; 12.3. analizează și propune măsurile tehnice sau organizatorice necesare în cazul apariției unor dificultăți în schimbul de informații; 12.4. contribuie la clarificarea și armonizarea procedurilor operaționale de schimb de date și informații în conformitate cu standardele europene; 12.5. 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	Compatibil	

	extind asupra metodelor și celor mai bune practici de prevenire și nu includ date cu caracter personal.		
Articolul 18. Statistici (1) Până la data de 1 martie a fiecărui an, fiecare stat membru furnizează Comisiei statistici privind schimburile de informații cu alte state membre în temeiul prezentei directive care au avut loc în anul calendaristic precedent.	<i>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</i> Anexa nr.1 Punctul 12. 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.	Compatibil	
(2) Fiecare stat membru se asigură că statisticile menționate la alineatul (1) acoperă cel puțin: (a) numărul de cereri de informații transmise de punctul lor de contact unic și, după caz, de autoritățile lor competente de aplicare a legii; (b) numărul de cereri de informații care au fost primite și numărul de cereri de informații la care s-a răspuns de către punctul lor de contact unic și de către autoritățile lor competente de aplicare a legii, defalcate pe cereri urgente și neurgente și defalcate în funcție de fiecare stat membru care a solicitat informațiile; (c) numărul de cereri de informații cărora nu li s-a dat curs în temeiul articolului 6, defalcate în funcție de state membre solicitante și în funcție de motivele de refuz; (d) numărul de cazuri în care s-au înregistrat abateri de la termenele prevăzute la articolul 5 alineatul (1) din cauza obligației de a obține o autorizație	<i>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</i> Anexa nr.1 Punctul 13. Această raportare vizează exclusiv managementul informațiilor și cuprinde: 113.1. numărul de cereri de informații transmise și primite; 113.2. numărul de răspunsuri furnizate, defalcate în cereri urgente și neurgente; 113.3. numărul de cereri refuzate și motivele aferente; 113.4. statisticile privind respectarea termenelor de 8 ore/3 zile/7 zile și impactul autorizațiilor judiciare asupra acestora.	Compatibil	

judiciară în conformitate cu articolul 5 alineatul (2), defalcate în funcție de statele membre care au transmis cererile de informații în cauză.			
(3) Comisia compilează statisticile minime furnizate de statele membre în temeiul alineatului (2) și le pune la dispoziția Parlamentului European și a Consiliului.		Prevedere UE neaplicabilă	Prevederea reglementează obligația Comisiei către Parlamentul European și Consiliu de a compila statisticile.
Articolul 19. Raportare (1) Până la 12 iunie 2026 și, ulterior, la fiecare cinci ani după 12 iunie 2027, Comisia prezintă Parlamentului European și Consiliului un raport de evaluare a punerii în aplicare a prezentei directive, cu informații detaliate privind punerea în aplicare a prezentei directive în fiecare stat membru. La întocmirea raportului respectiv, Comisia acordă o atenție deosebită eficienței schimbului de informații între autoritățile competente de aplicare a legii, motivelor pentru care au fost refuzate cererile de informații, în special în cazul în care cererile nu intră în sfera de aplicare a obiectivelor prezentei directive, precum și respectării dispozițiilor privind protecția datelor și furnizarea de informații către Europol.		Prevedere UE neaplicabilă	Prevederea reglementează obligația de raportare a Comisiei către Parlamentul European și Consiliu (mecanism UE de evaluare/monitorizare instituțională).
Articolul 20. Modificarea Convenției de punere în aplicare a Acordului Schengen De la 12 decembrie 2024, acele părți din articolele 39 și 46 din Convenția de punere în aplicare a Acordului Schengen care nu au fost înlocuite de Decizia-cadru 2006/960/JAI se înlocuiesc cu prezenta directivă în măsura în care articolele		Prevedere UE neaplicabilă	

respective se referă la schimbul de informații care intră în domeniul de aplicare al prezentei directive.			
Articolul 21. Abrogare Decizia-cadru 2006/960/JAI se abrogă de la 12 decembrie 2024. Trimiterile la decizia-cadru abrogată se interpretează ca trimiteri la prezenta directivă și se citesc în conformitate cu tabelul de corespondență din anexă.		Prevedere UE neaplicabilă	
Articolul 22. Transpunere (1) Statele membre asigură intrarea în vigoare a actelor cu putere de lege și a actelor administrative necesare pentru a se conforma prezentei directive până la 12 decembrie 2024. Statele membre informează de îndată Comisia cu privire la aceasta. Prin derogare de la primul paragraf, statele membre asigură intrarea în vigoare a actelor cu putere de lege și a actelor administrative necesare pentru a se conforma articolului 13 până la 12 iunie 2027. Statele membre informează de îndată Comisia cu privire la aceasta. Atunci când statele membre adoptă dispozițiile menționate la primul și la al doilea paragraf, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a unei astfel de trimiteri. (2) Comisiei îi sunt comunicate de către statele membre textele principalelor dispoziții de drept intern pe care le adoptă în domeniul reglementat de prezenta directivă.		Prevedere UE neaplicabilă	

Articolul 23. Intrarea în vigoare Prezenta directivă intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene.		Prevedere UE neaplicabilă	
Articolul 24. Destinatari Prezenta directivă se adresează statelor membre în conformitate cu tratatele.		Prevedere UE neaplicabilă	

TABEL DE CONCORDANȚĂ

a proiectului de Hotărâre 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.	Titlul actului UE, inclusiv cea mai recentă modificare, nr. CELEX: Poziția comună 2005/69/JAI a Consiliului din 24 ianuarie 2005 privind schimbul de anumite date cu Interpol		
2.	Titlul proiectului de act normativ național: Proiect de Hotărâre 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		
3.	Gradul general de compatibilitate compatibil		
4.	Autoritatea/persoana responsabilă Ministerul Afacerilor Interne		
5.	Data întocmirii/actualizării 15.05.2026		
6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observații
Articolul 1. Obiect Obiectul prezentei poziții comune constă în prevenirea și combaterea criminalității grave și organizate, inclusiv a terorismului, asigurând că statele membre iau măsurile necesare pentru întărirea cooperării între autoritățile lor competente, responsabile cu aplicarea legii, precum și între acestea și autoritățile omoloage din țări terțe, prin schimbul de date cu Interpol privind pașapoartele.	<i>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</i> Anexa nr.1 Punctul 1. Prezentul 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 (ADN, dactiloscopie, imagini faciale), date privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, evidențe ale poliției,	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 1. Obiectul de reglementare (2) Prezenta lege stabilește norme privind: b) schimbul de date cu privire la căutarea directă sau automatizată de profiluri ADN, date dactiloscopice, date privind vehicule precum și piesele componente ale acestuia consemnate cu număr de identificare, imagini faciale, date privind documente de călătorie declarate furate, pierdute, revocate, nevalidate sau blaturile documentelor sustrase înainte de emitere, evidențe ale poliției, datele personale ale persoanelor străine sau cetățenilor Republicii Moldova urmăriți internațional, aflați în vizorul autorităților de aplicare a legii, datele biometrice și antropometrice necesare identificării persoanelor dispărute fără veste, cadavrelor și părților acestuia, precum și alte date care fac obiectul schimbului de date de interes polițienesc;

	date care nu privesc persoanele și informații operative, documente de călătorie, vizele, titlurile de valoare, inclusiv a celor declarate false, furate sau pierdute, precum și date privind permisele de conducere. Anexa nr.2 Punctul 1. Prezentul Regulament stabilește cadrul normativ pentru organizarea, funcționarea și atribuțiile Punctelor Naționale de Contact (<i>în continuare – PNC</i>), precum și procedurile operaționale pentru schimbul de date biometrice (ADN, dactiloscopie, imagini faciale), date privind vehiculele, evidențe ale poliției, documente de călătorie furate, pierdute, revocate, nevalidate sau blancurile documentelor furate înainte de emitere, precum și date privind permisele de conducere. Punctul 62. ASP este desemnată în calitate de PNC responsabil de gestionarea bazelor de date naționale privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, a datelor referitoare la documente de călătorie, vizele, titlurile de valoare, 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.		
Articolul 2. Definiții În sensul prezentei poziții comune, se aplică următoarele definiții: 1. „Date privind pașapoartele” înseamnă date privind pașapoartele emise și necompletate, care au fost furate, pierdute sau sustrase în alt mod și care sunt formatate pentru a fi introduse într-un sistem de informații specific. Datele privind pașapoartele care fac obiectul unor schimburi cu baza de date Interpol cuprind numai numărul pașaportului, țara emitentă și tipul documentului.		Compatibil	<i>Legea nr. 273 din 09.11.1994 privind actele de identitate din sistemul național de pașapoarte</i> Articolul 2. Pașaportul, documentele de călătorie (5) Pașaportul și documentele de călătorie conțin următoarele date în format tipărit și în format inscripționat pe cardul integrat de date de identificare: a) denumirea statului emitent în limbile română, engleză și franceză; b) codul statului emitent; c) denumirea actului de identitate în limbile română, engleză și franceză; d) tipul actului de identitate (codul); e) seria și numărul; f) numele; g) prenumele; h) cetățenia. Informația cu privire la cetățenie nu se înscrie în documentele de călătorie; i) data nașterii; j) numărul de identificare de stat al persoanei fizice; k) sexul; l) locul nașterii (țara de origine); m) data emiterii; n) autoritatea emitentă; o) data expirării termenului de valabilitate; p) imaginea facială; q) semnătura olografă a titularului, care se aplică de la vârsta de 14 ani. În cazul persoanelor cu vârsta sub 14 ani și

			al celor care nu pot aplica semnătura olografă, se aplică o mențiune specială în condițiile stabilite de către Guvern. <i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 23. Date privind documentele de călătorie raportate ca fiind pierdute, furate, nevalidate sau falsificate (2) Datele prelucrate nu includ informații care permit identificarea directă a titularului documentului de călătorie, fiind strict limitate la date tehnice esențiale pentru identificarea documentului și pentru cooperarea polițienească internațională. (3) Setul de date prelucrate cuprinde următoarele informații: a) numărul documentului de călătorie; b) denumirea statului emitent al documentului de călătorie; c) tipul documentului (pașaport, pașaport diplomatic, pașaport de serviciu, document de călătorie); d) data și circumstanțele cunoscute despre declararea documentului de călătorie ca fiind pierdut, sustras, nevalidat sau falsificat (inclusiv autoritatea care a emis notificarea).
2. „Baza de date Interpol” înseamnă baza de date cu sistem de căutare automată privind documentele de călătorie furate, gestionată de Organizația Internațională de Poliție Criminală – Interpol.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 3. Noțiuni generale 4) <i>baze de date INTERPOL</i> – ansamblul sistemelor informaționale și al registrelor centralizate, gestionate de Secretariatul General al Organizației Internaționale a Poliției Criminale (INTERPOL), care conțin date cu caracter personal, date biometrice (profiluri ADN, date dactiloscopice, imagini faciale, ș.a) și informații operative privind obiecte, documente sau activități infracționale, puse la dispoziția statelor membre în scopul schimbului de informații pentru prevenirea și combaterea criminalității transfrontaliere;

3. „Bază de date națională relevantă” înseamnă baza de date sau bazele de date ale autorităților polițienești sau judiciare ale unui stat membru care conțin date privind pașapoartele emise sau necompletate care au fost furate, pierdute sau sustrase în alt mod.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 3. Noțiuni generale 4) <i>baze de date naționale</i> – ansamblul sistemelor informaționale gestionate de către autoritățile competente ale Republicii Moldova, accesate în scopul implementării prezentei legi;
Articolul 3. Acțiunea comună (1) Autoritățile competente ale statelor membre, responsabile cu aplicarea legii, schimbă cu Interpol toate datele deja existente și viitoare privind pașapoartele. Aceste date sunt accesibile altor membri Interpol numai în măsura în care aceștia asigură un nivel adecvat de protecție a datelor personale. De asemenea, se asigură respectarea drepturilor și libertăților fundamentale cu privire la prelucrarea automată a datelor personale. Statele membre pot decide să permită accesul la datele de care dispun numai altor membri Interpol care s-au angajat să schimbe cel puțin aceleași date.	<i>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</i> Anexa nr.1 Punctul 9. Structura internă a PUC include următoarele subdiviziuni specializate ale DCPI: 9.2. <i>Biroul Național Central Interpol</i> – asigură interfața cu baza de date SLTD privind documente de călătorie, vizele, titlurile de valoare, inclusiv a celor declarate false, furate sau pierdute, precum și a datelor privind permisele de conducere; Anexa nr.2 Punctul 62. ASP este desemnată în calitate de PNC responsabil de gestionarea bazelor de date naționale privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 24. Schimbul de date privind documentele de călătorie raportate ca fiind pierdute, furate, nevalidate sau falsificate (1) Autoritatea competentă asigură transmiterea datelor privind documentele de călătorie raportate ca fiind pierdute, furate, nevalidate sau falsificate prin sistemul automatizat de schimb de date cu baza de date SLTD al secretariatului general INTERPOL, cu respectarea cerințelor de protecție a datelor cu caracter personal.

	faptelor ilegale, a datelor referitoare la documente de călătorie, vizele, titlurile de valoare, 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. Punctul 64. ASP asigură lansarea și primirea interogărilor automatizate fără întârziere, garantând accesul autorităților competente la datele privind proprietarii de vehicule și statutul documentelor de călătorie. 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.		
(2) Sub rezerva cerințelor formulate la alineatul (1), fiecare stat membru poate conveni cu Interpol modalitățile de schimb al datelor existente privind pașapoartele de care dispune cu Interpol. Aceste date sunt cuprinse în baza de date națională relevantă sau în SIS,	<i>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</i> Anexa nr.2 Punctul 65. ASP asigură interfața tehnică și fluxul de date necesar pentru	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 24. Schimbul de date privind documentele de călătorie raportate ca fiind pierdute, furate, nevalidate sau falsificate (2) Introducerea și actualizarea datelor în baza de date SLTD al secretariatului general INTERPOL se realizează în mod direct și automat de către autoritățile competente care dețin acces la sistem, iar în cazuri de nefuncționare a

în cazul în care participă la acesta.	introducerea și gestionarea în Sistemul de Informații Schengen (SIS) a alertelor referitoare la mijloacele de transport și documente (de călătorie, certificate de înmatriculare și permise de conducere) raportate ca fiind furate, pierdute, sustrase sau anulate.		acestui, schimbul de date este asigurat în regim manual prin intermediul canalelor securizate gestionate de subdiviziunea specializată în cooperare polițienească internațională din subordinea Inspectoratului General al Poliției al Ministerului Afacerilor Interne.
(3) Fiecare stat membru asigură că, imediat după ce s-au introdus date în baza sa de date națională relevantă sau în SIS, în cazul în care participă la acesta, datele respective sunt schimbate și cu Interpol.	<i>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</i> Anexa nr.2 Punctul 62. ASP este desemnată în calitate de PNC responsabil de gestionarea bazelor de date naționale privind mijloacele de transport, date referitoare la autovehiculele anunțate în căutare, precum și piesele componente identificabile ale acestora urmărite internațional sau fiind obiecte ale faptelor ilegale, a datelor referitoare la documente de călătorie, vizele, titlurile de valoare, 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	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 24. Schimbul de date privind documentele de călătorie raportate ca fiind pierdute, furate, nevalidate sau falsificate (3) Transmiterea și introducerea datelor se efectuează într-un termen rezonabil, în vederea asigurării accesului statelor membre la informații actualizate privind documentele de călătorie semnalate. (4) Autoritățile competente asigură exactitatea și actualizarea datelor, precum și radierea acestora în cazul în care temeiul semnalării a încetat, în conformitate cu procedurile naționale și internaționale.

	SLTD a Interpol pentru verificarea documentelor de călătorie.		
(4) Statele membre asigură că autoritățile lor competente responsabile cu aplicarea legii consultă baza de date Interpol, în sensul prezentei poziții comune, de fiecare dată când acest lucru este necesar pentru îndeplinirea sarcinilor ce le revin. Statele membre asigură instituirea infrastructurilor necesare pentru a facilita consultarea datelor de îndată ce acest lucru este posibil, dar cel târziu până în decembrie 2005.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 25. Căutarea automatizată a datelor privind documentele de călătorie raportate ca fiind pierdute, furate, nevalidate sau falsificate (1) Autoritățile competente pentru verificarea documentelor de călătorie efectuează verificări automatizate în baza de date SLTD, prin intermediul infrastructurii puse la dispoziție de INTERPOL. (2) Verificarea se realizează, în special, cu ocazia controlului la trecerea frontierei de stat, precum și în alte situații prevăzute de lege. (3) În cazul obținerii unei concordanțe pozitive („hit”), autoritatea competentă: a) verifică exactitatea datelor; b) confirmă informația prin intermediul subdiviziunii specializată în cooperare polițienească internațională din subordinea Inspectoratului General al Poliției al Ministerului Afacerilor Interne.
(5) Schimbul de date personale, în conformitate cu obligația prevăzută de prezenta poziție comună, are loc în scopul prevăzut la articolul 1, asigurându-se un nivel adecvat de protecție a datelor personale în respectiva țara membră Interpol, precum și respectarea drepturilor și libertăților fundamentale privind prelucrarea automată a datelor personale. În acest scop, statele membre asigură că schimbul și partajarea datelor au loc în	<i>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 Anexa nr.1</i> Punctul 6. PUC își desfășoară activitatea în conformitate cu următoarele principii generale stabilite pentru activitatea Poliției: 6.2. <i>supremația legii, respectarea drepturilor și libertăților fundamentale ale omului</i> - schimbul de informații este limitat la prevenirea și investigarea infracțiunilor, respectând strict	Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 5. Garanții privind protecția datelor cu caracter personal (1) Prelucrarea datelor cu caracter personal în temeiul prezentei legi se limitează la datele strict necesare realizării scopurilor prevăzute de aceasta. (2) Datele obținute prin sistemul de schimb automatizat nu pot fi utilizate în alte scopuri decât cele pentru care au fost solicitate și furnizate.

condiții adecvate și sub rezerva condițiilor menționate anterior.	necesitatea, proporționalitatea și protecția datelor personale; Punctul 90. Prelucrarea datelor cu caracter personal se realizează în conformitate cu legislația națională privind protecția datelor și cu standardele Uniunii Europene aplicabile în domeniul cooperării polițienești.		
(6) În cazul în care în baza de date Interpol se ajunge la o identificare pozitivă, fiecare stat membru asigură că autoritățile sale competente iau măsuri în conformitate cu legislația națională, de exemplu verifică, după caz, corectitudinea datelor, împreună cu țara care a introdus datele.		Compatibil	<i>Proiectul de lege privind cooperarea polițienească internațională</i> Articolul 25. Căutarea automatizată a datelor privind documentele de călătorie raportate ca fiind pierdute, furate, nevalidate sau falsificate (1) Autoritățile competente pentru verificarea documentelor de călătorie efectuează verificări automatizate în baza de date SLTD, prin intermediul infrastructurii puse la dispoziție de INTERPOL. (2) Verificarea se realizează, în special, cu ocazia controlului la trecerea frontierei de stat, precum și în alte situații prevăzute de lege. (3) În cazul obținerii unei concordanțe pozitive („hit”), autoritatea competentă: a) verifică exactitatea datelor; b) confirmă informația prin intermediul Biroului Național Central INTERPOL.
Articolul 4. Monitorizarea și evaluarea Pe baza informațiilor furnizate de statele membre, până în decembrie 2005 Comisia prezintă Consiliului un raport cu privire la punerea în aplicare a prezentei poziții comune. Consiliul evaluează în ce măsură statele membre respectă prezenta poziție		Prevederi UE neaplicabile	

comună și ia măsurile corespunzătoare.			
Articolul 5. Intrare în vigoare Prezenta poziție comună intră în vigoare la data adoptării sale.		Prevederi UE neaplicabile	
Articolul 6. Publicare Prezenta poziție comună se publică în Jurnalul Oficial al Uniunii Europene.		Prevederi UE neaplicabile	



Nr. 38/2049 din 20 mai 2026

Cancelaria de Stat

CERERE
privind înregistrarea de către Cancelaria de Stat
a proiectelor de acte ale Guvernului

Nr. crt.	Criterii de înregistrare	Nota autorului
1.	Categoria și denumirea proiectului	Proiectul hotărârii Guvernului cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații.
2.	Autoritatea care a elaborat proiectul	Ministerul Afacerilor Interne.
3.	Justificarea depunerii cererii	Proiectul menționat a fost elaborat în scopul realizării angajamentului asumat prin Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029, aprobat prin Hotărârea Guvernului nr. 306/2025, cu modificările ulterioare.
4	Referința la documentul de planificare care prevede elaborarea proiectului (<i>PNA, PND, PNR, alte documente de planificare sectoriale</i>)	Inițierea acestui proiect de act normativ rezidă din acțiunile operaționale nr. 53, 58 și 66 din Clusterul 1. Valori fundamentale, Capitolul 24 „Justiție, libertate și Securitate” al Programului național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029, aprobat prin Hotărârea Guvernului nr. 306/2025.
5.	Lista autorităților și instituțiilor a căror avizare este necesară	1. Cancelaria de Stat (Centrul de Armonizare a Legislației); 2. Ministerul Justiției/Centrul Național de Expertiză Judiciară; 3. Serviciul de Informații și Securitate; 4. Procuratura Generală; 5. Consiliul Superior al Magistraturii; 6. Ministerul Afacerilor Externe;

		7. Ministerul Finanțelor (Serviciul Vamal); 8. Ministerul Dezvoltării Economice și Digitalizării; 9. Agenția Servicii Publice; 10. Serviciul Tehnologia Informației și Securitate Cibernetică; 11. Agenția de Guvernare Electronică; 12. Centrul Național pentru Protecția Datelor cu Caracter Personal. Expertiza juridică: Ministerul Justiției. Expertiza anticorupție: Centrul Național Anticorupție. Expertiza de compatibilitate cu legislația UE: Centrul de armonizare a legislației.
6.	Termenul-limită pentru depunerea avizelor/expertizelor	10 zile.
7.	Persoana responsabilă de promovarea proiectului	Irina Dragoman, ofițer principal al Secției politici în domeniul combaterii criminalității a Direcția politici în domeniul ordinii și securității publice, combaterii criminalității. tel: 0 22 255-750, 069552472 e-mail: irina.dragoman@mai.gov.md
8.	Anexe	1. Proiectul actului normativ; 2. Nota de fundamentare la proiect; 3. Tabelele de concordanță ale actelor UE: 3.1. 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); 3.2. Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în

		domeniul combaterii terorismului și a criminalității transfrontaliere; 3.3. 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; 3.4. Decizia 2004/919/CE a Consiliului din 22 decembrie 2004 privind combaterea criminalității referitoare la vehicule și având implicații transfrontaliere; 3.5. Poziția comună 2005/69/JAI a Consiliului din 24 ianuarie 2005 privind schimbul de anumite date cu Interpol.
9.	Data și ora depunerii cererii	Conform semnăturii electronice
10.	Semnat electronic	Ministrul afacerilor interne Daniella MISAIL-NICHITIN

Executor: Dragoman Irina
 Telefon: 022-255-750
 E-mail: irina.dragoman@mai.gov.md