Proiect
UE

GUVERNUL REPUBLICII MOLDOVA
HOTĂRÂRE nr. _____
din _____ 2026
mun. Chișinău

cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale

---

În temeiul art. 22 lit. d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), cu modificările ulterioare, art. 16 alin. (3) și art. 19 alin.(1) din Legea nr. 71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70-73, art. 314), cu modificările ulterioare, art. 6 lit. h) din Legea nr. 136/2017 cu privire la Guvern (Monitorul Oficial al Republicii Moldova, 2017, nr. 252, art. 412), cu modificările ulterioare, Guvernul HOTĂRĂȘTE:

Prezenta hotărâre transpune parțial (transpune: art. 19, art. 20, art. 21, art. 22 alin. (1), art. 24 alin. (1) și (2)) 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.

1. Se instituie Sistemul informațional „Registrul imaginilor faciale”.
2. Se aprobă:
2.1. Conceptul Sistemului informațional „Registrul imaginilor faciale”, conform anexei nr. 1;
2.2. Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale, conform anexei nr. 2.
3. Ministerul Afacerilor Interne va asigur condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea Sistemului informațional „Registrul imaginilor faciale”.
4. Prevederile prezentei hotărâri referitoare la constituirea, utilizarea și schimbul automatizat transfrontalier al setului de date de referință privind imaginile faciale se aplică de la data intrării în vigoare a actului normativ privind cooperarea polițienească internațională și după îndeplinirea condițiilor juridice, organizatorice și tehnice prevăzute de aceasta, inclusiv efectuarea notificărilor, desemnarea punctelor de contact și operaționalizarea mecanismelor externe aplicabile.
5. Prezenta hotărâre intră în vigoare la expirarea termenului 6 luni de la data publicării în Monitorul Oficial al Republicii Moldova, cu excepția prevederilor menționate la pct. 4, care se aplică în condițiile stabilite la punctul respectiv.
6. Controlul asupra executării prezentei hotărâri se pune în sarcină Ministerului Afacerilor Interne.

PRIM-MINISTRU **ALEXANDRU MUNTEANU**

Contrasemnează:
Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării Eugen Osmochescu

Ministrul afacerilor interne Daniella Misail-Nichitin

Anexa nr. 1
aprobată prin Hotărârea Guvernului
nr._____/ 2026

CONCEPTUL
Sistemului informațional „Registrul imaginilor faciale”

Capitolul I. Introducere

1. Prezentul Concept stabilește cadrul general de creare, dezvoltare și funcționare a Sistemului informațional „Registrul imaginilor faciale” (în continuare – SI RIF).

2. SI RIF se instituie în scopul asigurării suportului informațional necesar autorităților competente pentru prelucrarea imaginilor faciale, identificarea biometrică facială și schimbul automatizat al datelor de referință privind imaginile faciale, în condițiile cadrului normativ aplicabil cooperării polițienești internaționale și tratatelor internaționale.

3. Crearea SI RIF este determinată de necesitatea consolidării capacităților naționale în domeniul prevenirii, constatării și investigării infracțiunilor, identificării ori verificării identității persoanelor, căutării persoanelor dispărute și identificării cadavrelor ori a părților acestora, precum și al cooperării polițienești internaționale, inclusiv în contextul armonizării cadrului normativ național cu actele relevante ale Uniunii Europene în materia căutării și schimbului automatizat de date.

4. SI RIF este conceput ca sistem informațional distinct, specializat în evidența, compararea biometrică facială, validarea concordanțelor și gestionarea imaginilor faciale, interoperabil cu sistemele informaționale și resursele informaționale relevante ale statului, fără a substitui funcțiile de evidență primară ale acestora.

5. Prezentul Concept definește scopul, obiectivele, principiile de funcționare, structura generală, categoriile de subiecți implicați, cerințele generale de interoperabilitate și securitate, constituind fundamentul pentru adoptarea Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale.

Capitolul II. Dispoziții generale

6. SI RIF este un sistem informațional distinct, specializat, constituit din resurse informaționale, tehnologii informaționale interdependente, metode și personal, destinat formării, administrării, păstrării, prelucrării, furnizării și utilizării informațiilor privind imaginile faciale și datele de referință privind imaginile faciale, inclusiv pentru realizarea schimbului automatizat al datelor de referință privind imaginile faciale, în condițiile legii, ale cadrului normativ aplicabil cooperării polițienești internaționale și ale tratatelor internaționale.

7. Registrul imaginilor faciale reprezintă resursa informațională departamentală de stat, specializată, ținută în formă electronică prin intermediul SI RIF, care cuprinde imagini faciale, date de referință privind imaginile faciale, metadate aferente, precum și informații privind rezultatele comparării automatizate.

8. În Registrul imaginilor faciale se introduc imagini faciale identificate și imagini faciale neidentificate, obținute din surse autorizate, precum și datele de referință aferente acestora. Imaginile faciale neidentificate se marchează și se recunosc ca atare.

9. Fiecărei imagini faciale introduse în Registrul imaginilor faciale i se atribuie un număr de referință, utilizat ca identificator al obiectului informațional și ca element de legătură pentru extragerea, după caz, a datelor de bază și a informațiilor suplimentare în cazul unei concordanțe confirmate.

10. În cadrul SI RIF se disting, din punct de vedere funcțional și juridic:

10.1. componenta națională a Registrului imaginilor faciale, care cuprinde totalitatea imaginilor faciale, a metadatelor aferente, a informațiilor asociate, a rezultatelor comparării

automatizate și a altor date necesare realizării atribuțiilor autorităților competente, în condițiile legii;

10.2. setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier, care reprezintă o submulțime distinctă a datelor gestionate prin SI RIF și care este constituit, păstrat, furnizat și utilizat exclusiv în condițiile legii și ale tratatelor internaționale aplicabile;

10.3. setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier se constituie numai pentru categoriile de persoane care au calitatea de bănuit, învinuit, inculpat, condamnat pentru săvârșirea infracțiunilor, precum și, după caz, ale victimei, în măsură în care cadrul normativ național permite acest lucru.

10.4. imaginile faciale aferente persoanelor dispărute fără veste, cadavrelor ori părților acestora pot fi gestionate în componenta națională a Registrului imaginilor faciale, în condițiile legii, exclusiv pentru realizarea atribuțiilor autorităților competente privind căutarea persoanelor dispărute și identificarea cadavrelor ori a părților acestora, fără a fi incluse în setul de date de referință destinat schimbului automatizat transfrontalier.

11. Datele de referință privind imaginile faciale puse la dispoziție prin intermediul SI RIF nu conțin date suplimentare care permit identificarea directă a persoanei. Datele de identificare ale persoanei și alte informații suplimentare pot fi extrase și furnizate numai ulterior confirmării concordanței și numai în condițiile legii.

12. În sensul prezentului Concept, termenii utilizați au următoarele semnificații:

12.1. imagine facială – imagine digitală a feței;

12.2. date de referință privind imaginile faciale – imagine facială și numărul de referință aferent, utilizate pentru compararea și schimbul automatizat transfrontalier al datelor, fără a permite identificarea directă a persoanei;

12.3. set de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier – totalitatea distinctă a datelor de referință extrase din SI RIF și puse la dispoziție pentru căutare automatizată transfrontalieră, în condițiile legii;

12.4. imagine facială identificată – imaginea facială a unei persoane identificate;

12.5. imagine facială neidentificată – imagine facială colectată în cursul prevenirii, constatării sau investigării unei infracțiuni ori în cadrul căutării unei persoane dispărute sau al identificării cadavrelor ori a unor părți ale acestora, care nu sunt asociate, la momentul introducerii, unei persoane identificate;

12.6. număr de referință – identificator alfanumeric unic atribuit imaginii faciale, care include elementele tehnice prevăzute de lege și de documentația tehnică aplicabilă, inclusiv, după caz, codul statului, identificatorul unic al imaginii faciale și indicatorul privind caracterul identificat sau neidentificat al imaginii, fără a conține date care permit identificarea directă a persoanei;

12.7. concordanță confirmată – corespondență dintre două sau mai multe imagini faciale, stabilită în urma comparării automatizate și confirmată prin validare de către personal calificat, în condițiile legii;

12.8. caz individual – situație concretă, individualizată și documentată potrivit legii, legată de prevenirea, constatarea sau investigarea unei infracțiuni, de căutarea unei persoane dispărute ori de identificarea unor cadavre sau a părților acestora;

12.9. validarea concordanței – verificarea rezultatului comparării automatizate de către personal calificat, în condițiile legii;

12.10. listă a mostrelor pentru care există posibilitatea unei concordanțe – rezultat tehnic intermediar al comparării automatizate, format din una sau mai multe mostre comparative selectate de SI RIF în baza nivelului de asemănare determinat potrivit regulilor de procesare aplicabile, care nu constituie concordanță confirmată și nu produce efecte juridice, procesuale, operaționale sau administrative până la validarea concordanței de către personal calificat.

13. Scopul SI RIF constă în asigurarea suportului informațional și funcțional necesar autorităților competente pentru prelucrarea imaginilor faciale, identificarea biometrică facială,

validarea concordanțelor, precum și pentru constituirea și utilizarea, în condițiile legii, a setului de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier.

14. Obiectivele SI RIF sunt:

14.1. asigurarea unei evidențe electronice specializate a imaginilor faciale identificate și neidentificate, precum și a metadatelor și informațiilor asociate acestora, în cadrul componentei naționale a registrului;

14.2. asigurarea comparării automatizate a imaginilor faciale și a formării rezultatului tehnic preliminar al comparării, inclusiv, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe ori a rezultatului privind inexistența unei concordanțe posibile;

14.3. asigurarea validării, în condițiile legii, a rezultatului tehnic preliminar al comparării automatizate și, după caz, a concordanțelor posibile rezultate din aceasta;

14.4. constituirea distinctă, în cadrul SI RIF, a setului de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier;

14.5. asigurarea disponibilității setului de date de referință privind imaginile faciale pentru schimbul automatizat cu autoritățile competente străine și, după caz, cu alte entități abilitate prin lege, exclusiv în condițiile cadrului normativ aplicabil;

14.6. asigurarea interoperabilității cu sistemele informaționale și resursele informaționale relevante ale statului, fără a substitui funcțiile de evidență primară ale acestora;

14.7. asigurarea trasabilității operațiunilor de prelucrare, a accesului autorizat și diferențiat, precum și a securității informației și protecției datelor cu caracter personal;

14.8. consolidarea capacităților naționale în domeniul prevenirii, constatării și investigării infracțiunilor, al identificării persoanelor și al cooperării polițienești internaționale.

15. La proiectarea, dezvoltarea și implementarea SI RIF, în scopul asigurării realizării obiectivelor menționate, se respectă următoarele principii:

15.1. principiul legalității, potrivit căruia crearea, administrarea și utilizarea sistemului se realizează numai în temeiul și în limitele legii;

15.2. principiul necesității și proporționalității, potrivit căruia prelucrarea datelor se efectuează numai în măsura necesară realizării scopurilor legale;

15.3. principiul limitării scopului, potrivit căruia datele se prelucrează numai pentru scopurile pentru care sistemul a fost instituit;

15.4. principiul exactității și actualității datelor, potrivit căruia în registru se introduc și se mențin doar date corecte, relevante și actualizate;

15.5. principiul accesului autorizat și diferențiat, potrivit căruia accesul la date se acordă în funcție de competențe, roluri și necesitatea funcțională;

15.6. principiul delimitării funcționale a datelor, potrivit căruia componenta națională a registrului și setul de date de referință destinat schimbului automatizat transfrontalier sunt constituite, utilizate și administrate distinct, în condițiile legii;

15.7. principiul interoperabilității, potrivit căruia sistemul este proiectat și utilizat astfel încât să poată interacționa legal, semantic, organizatoric și tehnic cu alte sisteme și resurse informaționale relevante;

15.8. principiul securității informației, potrivit căruia datele sunt protejate prin măsuri tehnice și organizatorice adecvate, care asigură confidențialitatea, integritatea, disponibilitatea și reziliența sistemului;

15.9. principiul trasabilității, potrivit căruia toate operațiunile relevante efectuate în sistem sunt jurnalizate și pot fi verificate ulterior;

15.10. principiul separării și marcării datelor, potrivit căruia imaginile faciale identificate și imaginile faciale neidentificate sunt recunoscute și tratate distinct;

15.11. principiul validării umane a concordanței, potrivit căruia rezultatele comparării automatizate care produc efecte operaționale sunt supuse verificării de către personal calificat, în condițiile legii.

16. Căutarea automatizată a datelor de referință privind imaginile faciale în componenta de schimb automatizat transfrontalier se efectuează exclusiv în cazuri individuale, în condițiile legii.

Utilizarea datelor gestionate prin SI RIF pentru interogări generale, exploratorii, nedeterminate sau pentru crearea de profiluri discriminatorii este interzisă.

17. Modul de organizare și ținere a Registrului imaginilor faciale, delimitarea dintre componenta națională a registrului și setul de date de referință destinat schimbului automatizat transfrontalier, categoriile de persoane eligibile pentru includerea în acest set, care sunt stabilite prin lege, categoriile de date, temeiurile de introducere, actualizare, rectificare, blocare, radiere și arhivare a datelor, condițiile de acces, comparare, validare, schimb automatizat, jurnalizare și control se stabilesc prin Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale, aprobat prin prezenta hotărâre.

Capitolul III. Spațiul juridico-normativ al funcționării sistemului

18. Funcționarea SI RIF se realizează în temeiul Constituției Republicii Moldova, al tratatelor internaționale la care Republica Moldova este parte, al cadrului normativ național aplicabil în domeniul resurselor informaționale de stat, registrelor, interoperabilității, protecției datelor cu caracter personal, securității cibernetice și activității autorităților competente, luându-se în considerare, la elaborarea și dezvoltarea sistemului, actele Uniunii Europene relevante în domeniu.

19. Cadrul normativ aplicabil creării, dezvoltării, administrării și funcționării SI RIF include:

19.1. Codul penal al Republicii Moldova nr. 985/2002;

19.2. Codul de procedură penală al Republicii Moldova nr. 122/2003;

19.3. Legea nr. 273/1994 privind actele de identitate din sistemul național de pașapoarte;

19.4. Legea nr. 1549/2002 cu privire la înregistrarea dactiloscopică de stat;

19.5. Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;

19.6. Legea nr. 216/2003 cu privire la Sistemul informațional integrat automatizat de evidență a infracțiunilor, a cauzelor penale și a persoanelor care au săvârșit infracțiuni;

19.7. Legea nr. 71/2007 cu privire la registre;

19.8. Legea nr. 195/2024 privind protecția datelor cu caracter personal;

19.9. Legea nr. 320/2012 privind activitatea Poliției și statutul polițistului;

19.10. Legea nr. 288/2016 privind funcționarul public cu statut special din cadrul Ministerului Afacerilor Interne;

19.11. Legea integrității nr. 82/2017;

19.12. Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară;

19.13. Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;

19.14. Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;

19.15. Legea nr. 148/2023 privind accesul la informații de interes public;

19.16. Legea nr. 48/2023 privind securitatea cibernetică;

19.17. Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;

19.18. Hotărârea Guvernului nr. 1202/2006 privind aprobarea Concepției Sistemului informațional integrat al organelor de drept;

19.19. Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;

19.20. Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);

19.21. Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);

19.22. Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);

19.23. Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);

19.24. Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;

19.25. Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);

19.26. Hotărârea Guvernului nr. 547/2019 cu privire la organizarea și funcționarea Inspectoratului General al Poliției;

19.27. Hotărârea Guvernului nr. 317/2020 cu privire la organizarea și funcționarea Serviciului Tehnologii Informaționale;

19.28. Hotărârea Guvernului nr. 375/2020 pentru aprobarea Conceptului Sistemului informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice" (MPower) și a Regulamentului privind modul de ținere a Registrului împuternicirilor de reprezentare în baza semnăturii electronice;

19.29. Hotărârea Guvernului nr. 376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify);

19.30. Hotărârea Guvernului nr. 153/2021 pentru aprobarea Conceptului Sistemului informațional „Registrul resurselor și sistemelor informaționale de stat" și a Regulamentului privind modul de ținere a Registrului resurselor și sistemelor informaționale de stat;

19.31. Hotărârea Guvernului nr. 323/2021 pentru aprobarea Conceptului Sistemului informațional „Catalogul semantic" și a Regulamentului privind modul de ținere a Registrului format de Sistemul informațional „Catalogul semantic";

19.32. Hotărârea Guvernului nr. 650/2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030;

19.33. Hotărârea Guvernului nr. 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice;

19.34. Hotărârea Guvernului nr. 677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design.

20. SI RIF se instituie în contextul alinierii cadrului normativ la exigențele privind căutarea și schimbul automatizat de date în scopul cooperării polițienești, în partea referitoare la imaginile faciale, prevăzute de 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).

21. Crearea și funcționarea eficientă a SI RIF necesită aprobarea și ajustarea actelor normative subsecvente care reglementează raporturile juridice aferente colectării, prelucrării, stocării, actualizării, comparării, validării și utilizării imaginilor faciale și a datelor de referință privind imaginile faciale, cu respectarea cadrului legal în domeniul protecției datelor cu caracter personal, securității informației și securității cibernetice.

Capitolul IV. Spațiul funcțional al SI RIF
Procesele și funcțiile SI RIF

22. Spațiul funcțional al SI RIF cuprinde totalitatea componentelor funcționale, proceselor informaționale și mecanismelor tehnice necesare pentru colectarea, recepționarea, evidența, stocarea, actualizarea, compararea, validarea, utilizarea și schimbul automatizat al datelor de referință privind imaginile faciale.

23. SI RIF include următoarele componente funcționale de bază:

23.1. componenta de recepționare și administrare a imaginilor faciale și a datelor de referință;

23.2. componenta de repozitoriu al datelor comparative privind imaginile faciale;

23.3. componenta de comparare biometrică facială;

23.4. componenta de suport al identificării cazului sau persoanei;

23.5. componenta de validare a concordanței;

23.6. componenta de interoperabilitate cu sistemele informaționale și resursele informaționale naționale relevante;

23.7. componenta de interoperabilitate cu sistemele informaționale externe utilizate în cooperarea polițienească internațională;

23.8. componenta de administrare, securitate, jurnalizare și audit.

24. Componenta de recepționare și administrare a imaginilor faciale și a datelor de referință asigură:

24.1. recepționarea imaginilor faciale din surse autorizate;

24.2. verificarea formală și tehnică a datelor recepționate;

24.3. înregistrarea și clasificarea datelor;

24.4. marcarea distinctă a imaginilor faciale identificate și neidentificate;

24.5. atribuirea numărului de referință;

24.6. actualizarea, rectificarea, completarea, blocarea, radierea și arhivarea datelor.

25. Componenta de repozitoriu al datelor comparative privind imaginile faciale asigură formarea, stocarea și gestionarea mostrelor comparative și a metadatelor aferente, inclusiv prin colectarea sau preluarea datelor din sisteme și resurse informaționale interoperabile.

26. Componenta de comparare biometrică facială asigură compararea automatizată a imaginilor faciale cu datele comparative privind imaginile faciale disponibile, inclusiv prin mecanisme de tip 1:1 și 1:N, determinarea nivelului de asemănare, generarea rezultatului tehnic preliminar al comparării și, după caz, formarea listei mostrelor pentru care există posibilitatea unei concordanțe, fără ca nivelul de asemănare ori lista respectivă să constituie concordanță confirmată.

27. Componenta de suport al identificării cazului sau persoanei asigură extragerea și formarea datelor de bază și a informațiilor suplimentare necesare identificării persoanei și, după caz, individualizării cazului, în baza numărului de referință și a identificatorilor asociați, inclusiv prin interacțiunea cu sistemele-sursă interoperabile.

28. Componenta de validare a concordanței asigură verificarea de către personal calificat a rezultatului comparării automatizate și, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe, confirmarea sau infirmarea concordanței și înregistrarea rezultatului validării.

29. Componenta de interoperabilitate cu sistemele informaționale și resursele informaționale naționale relevante asigură schimbul de date prin intermediul platformei de interoperabilitate (MConnect), fără a substitui funcțiile de evidență primară ale acestora.

30. Componenta de interoperabilitate cu sistemele informaționale externe utilizate în cooperarea polițienească internațională asigură, în condițiile legii speciale privind cooperarea polițienească internațională, ale tratatelor internaționale și ale actelor de punere în aplicare aplicabile, constituirea, extragerea, furnizarea, recepționarea și schimbul automatizat al setului de date de referință privind imaginile faciale, transmiterea și recepționarea solicitărilor și răspunsurilor de căutare automatizată, precum și suportul tehnic pentru furnizarea ulterioară a datelor de bază și a informațiilor suplimentare numai după confirmarea concordanței.

31. Componenta de administrare, securitate, jurnalizare și audit asigură:

31.1. administrarea utilizatorilor, rolurilor și drepturilor de acces;

31.2. administrarea nomenclatoarelor și a metadatelor de sistem;

31.3. jurnalizarea operațiunilor efectuate în sistem;

31.4. monitorizarea utilizării sistemului;

31.5. aplicarea măsurilor tehnice și organizatorice de securitate;

31.6. auditul și trasabilitatea operațiunilor.

32. Procesele de bază realizate prin intermediul SI RIF includ:

32.1. colectarea și recepționarea imaginilor faciale și a datelor de referință privind imaginile faciale;

32.2. verificarea și prelucrarea inițială a datelor;

32.3. introducerea și actualizarea datelor în registru;

32.4. marcarea distinctă a imaginilor faciale identificate și neidentificate;

32.5. compararea automatizată a imaginilor faciale;

32.6. validarea concordanței;

32.7. extragerea, ulterior confirmării concordanței și în condițiile legii, a datelor de bază și a informațiilor suplimentare;

32.8. constituirea distinctă și actualizarea setului de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier;

32.9. schimbul automatizat transfrontalier al setului de date de referință și furnizarea informațiilor ulterioare concordanței confirmate, prin canale autorizate;

32.10. jurnalizarea, monitorizarea și auditul operațiunilor.

33. SI RIF asigură funcționalități care permit:

33.1. utilizarea imaginilor faciale conforme cerințelor minime de calitate stabilite potrivit cadrului normativ aplicabil și documentației tehnice a sistemului, pentru compararea automatizată;

33.2. delimitarea funcțională dintre componenta națională a registrului și setul de date de referință destinat schimbului automatizat transfrontalier;

33.3. limitarea schimbului automatizat la setul de date strict necesar;

33.4. utilizarea numerelor de referință;

33.5. păstrarea istoricului actualizărilor și a rezultatelor comparării;

33.6. utilizarea componentei de schimb automatizat transfrontalier numai în cazuri individuale;

33.7. prevenirea accesului neautorizat și a utilizării datelor în scopuri incompatibile cu cadrul normativ aplicabil și cu scopurile pentru care SI RIF a fost instituit.

34. Regulile detaliate privind constituirea și actualizarea setului de date de referință destinat schimbului automatizat transfrontalier, categoriile de persoane eligibile pentru includerea în acesta, fluxurile operaționale, rolurile utilizatorilor, condițiile de acces, procedurile de comparare, formarea și statutul listei mostrelor pentru care există posibilitatea unei concordanțe, validarea concordanței, jurnalizarea și schimbul de date se stabilesc prin Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale.

Capitolul V. Structura organizațională a SI RIF
Funcțiile de bază și subiecții SI RIF

35. Structura organizațională a SI RIF este constituită din ansamblul autorităților și entităților responsabile de crearea, deținerea, administrarea tehnică, exploatarea funcțională, furnizarea datelor, utilizarea autorizată, controlul și supravegherea prelucrării datelor gestionate prin sistem.

36. Subiecții SI RIF sunt:

36.1. proprietarul sistemului;

36.2. posesorul sistemului;

36.3. deținătorul sistemului;

36.4. administratorul tehnic al sistemului;

36.5. utilizatorii sistemului;

36.6. registratorii;

36.7. furnizorii de date;

36.8. destinatarii datelor.

37. Proprietarul SI RIF este statul, care își realizează dreptul de proprietate, gestionare și utilizare a datelor din acesta.

38. Posesor al SI RIF este Ministerul Afacerilor Interne, care asigură guvernanța instituțională a sistemului, coordonarea dezvoltării și utilizării acestuia, cooperarea dintre autoritățile participante, precum și, în condițiile legii, coordonarea instituțională a participării SI RIF la mecanismul de căutare și schimb automatizat transfrontalier al datelor de referință privind imaginile faciale.

39. Deținător al SI RIF este Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne, care asigură crearea, dezvoltarea, mentenanța aplicativă, funcționarea tehnică a aplicației, administrarea componentelor software, a bazelor de date, a interfețelor și a mecanismelor aplicative de securitate, jurnalizare, monitorizare și audit, precum și suportul tehnic necesar funcționării SI RIF, în limitele competențelor sale și în coordonare cu administratorul tehnic pentru aspectele ce țin de găzduire și infrastructura tehnologiilor informaționale.

40. Administrator tehnic al SI RIF este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, care în limitele competențelor stabilite, asigură administrarea tehnică a infrastructurii tehnologiilor informaționale aferente găzduirii SI RIF, mentenanța infrastructurii gestionate, măsurile de securitate cibernetică și suportul tehnic aferent serviciilor prestate, fără a interveni în administrarea funcțională a datelor gestionate prin SI RIF.

41. Utilizatorii SI RIF sunt persoane fizice desemnate de către registratori, furnizorii de date și destinatarii datelor, care au acces autorizat la sistem în baza unui rol specific atribuit, conform politicilor de securitate și control al accesului, în limitele competențelor legale și numai pentru scopurile prevăzute de lege și prezentul Concept.

42. Registratorii sunt persoane autorizate, desemnate în condițiile legii, care efectuează în SI RIF operațiuni de introducere, actualizare, rectificare, completare, blocare, radiere și arhivare a datelor, inclusiv marcarea imaginilor faciale neidentificate, atribuirea, verificarea și menținerea evidenței numerelor de referință, actualizarea metadatelor aferente, înregistrarea solicitărilor și răspunsurilor de căutare automatizată, consemnarea rezultatelor comparării automatizate și a confirmării ori infirmării concordanței, precum și actualizarea datelor relevante pentru componenta de schimb automatizat transfrontalier, în limitele competențelor stabilite de lege și numai pentru scopurile prevăzute de cadrul normativ aplicabil.

43. Registratorii desemnați pentru componenta de schimb automatizat transfrontalier operează numai în cazuri individuale, cu utilizarea numerelor de referință, cu respectarea cerințelor de validare, jurnalizare și trasabilitate, precum și a procedurilor privind solicitările și răspunsurile de căutare automatizată, în condițiile legii.

44. Furnizorii de date sunt autoritățile și entitățile care furnizează, în condițiile legii, date, imagini faciale, metadate ori alte informații necesare formării, completării și actualizării Registrului imaginilor faciale, inclusiv prin mecanisme de interoperabilitate, precum și, după caz, pentru constituirea și actualizarea setului de date de referință destinat schimbului automatizat transfrontalier, cu asigurarea legalității furnizării, exactității, actualității, relevanței, integrității și, după caz, a calității suficiente a imaginilor faciale pentru compararea automatizată.

45. Destinatarii datelor sunt autoritățile și entitățile care au dreptul legal de a accesa sau primi date din SI RIF pentru realizarea atribuțiilor ce le revin, în condițiile legii, inclusiv, după caz, pentru extragerea și furnizarea datelor de bază și a informațiilor suplimentare aferente unei concordanțe confirmate, prin canalele, procedurile și punctele de contact stabilite de cadrul normativ aplicabil schimbului automatizat transfrontalier de date, cu respectarea principiului accesului autorizat și diferențiat, a necesității funcționale, a jurnalizării și trasabilității operațiunilor, precum și a interdicției utilizării datelor pentru interogări generale, exploratorii sau în alte scopuri decât cele prevăzute de lege.

46. Atribuțiile, drepturile, obligațiile, condițiile de acces, procedurile de desemnare, responsabilitățile și delimitarea competențelor subiecților SI RIF se stabilesc prin Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale, prin actele normative aplicabile și prin actele administrative emise în temeiul acestora.

Capitolul VI. Documentele și datele SI RIF

47. În cadrul SI RIF se folosesc următoarele categorii de documente:

47.1. documente de intrare, care constituie sursa primară pentru introducerea datelor în sistem;

47.2. documente de ieșire, obținute în urma procesării și funcționării sistemului;

47.3. documente tehnologice, generate și utilizate pentru menținerea, exploatarea, securizarea și auditarea sistemului.

48. Documentele de intrare ale SI RIF sunt următoarele:

48.1. imaginile faciale recepționate din surse autorizate, în condițiile legii;

48.2. imaginile faciale prelevate sau captate în cadrul acțiunilor procesuale, al activității speciale de investigații sau al altor activități prevăzute de lege;

48.3. imaginile faciale extrase din materiale foto, video sau din alte suporturi informaționale obținute legal;

48.4. imaginile faciale recepționate în cadrul schimbului de date cu autoritățile competente naționale ori străine, în condițiile legii;

48.5. documentele și datele de intrare referitoare la persoanele identificate, în cazurile prevăzute de lege;

48.6. documentele și datele de intrare aferente imaginilor faciale neidentificate;

48.7. datele de referință privind imaginile faciale și metadatele aferente acestora;

48.8. documentele și datele privind sursa imaginii faciale, data și locul prelevării, captării ori extragerii acesteia;

48.9. documentele și datele privind temeiul legal al introducerii imaginii faciale în registru;

48.10. documentele și datele privind cauza penală, dosarul de căutare sau alt obiect informațional conex, după caz;

48.11. solicitările de căutare automatizată a datelor de referință privind imaginile faciale;

48.12. documentele și datele privind confirmarea sau infirmarea concordanței rezultate în urma comparării automatizate;

48.13. documentele și datele recepționate prin interoperabilitate din alte sisteme informaționale și resurse informaționale relevante ale statului;

48.14. formularele standardizate de evidență, completate potrivit indicatorilor și cerințelor prevăzute de prezentul Concept și ale Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale.

49. Documentele de ieșire ale SI RIF sunt următoarele:

49.1. răspunsurile la solicitările de căutare automatizată a datelor de referință privind imaginile faciale;

49.2. extrase individuale din Registrul imaginilor faciale, eliberate autorităților competente, în condițiile legii;

49.3. rapoartele operative privind rezultatele comparării automatizate și, după caz, privind confirmarea sau infirmarea concordanței;

49.4. datele de bază și informațiile suplimentare furnizate ulterior unei concordanțe confirmate, în condițiile legii;

49.5. seturile de date, mesajele și extrasele transmise altor sisteme informaționale de stat, prin platforma de interoperabilitate ori prin alte canale autorizate;

49.6. seturile de date, mesajele și extrasele transmise în cadrul cooperării polițienești internaționale, în condițiile legii, ale tratatelor internaționale și ale actelor de punere în aplicare;

49.7. rapoartele analitice și statistice privind utilizarea sistemului, volumul datelor procesate, rezultatele comparărilor și alte informații agregate permise de lege;

49.8. notele informative și rapoartele operative destinate autorităților competente, în limitele competențelor acestora.

50. Documentele tehnologice sunt documente utilizate pentru gestionarea proceselor interne, asigurarea trasabilității operațiunilor, menținerea securității și arhivarea activităților desfășurate în cadrul sistemului și includ următoarele:

50.1. registrele electronice de evidență a operațiunilor efectuate în sistem;

50.2. jurnalele operațiunilor de accesare și prelucrare a datelor;

50.3. înregistrările privind introducerea, actualizarea, rectificarea, completarea, blocarea, radierea și arhivarea datelor;

50.4. înregistrările privind rezultatele comparării automatizate;

50.5. înregistrările privind confirmarea sau infirmarea concordanței;

50.6. jurnalele de acces și evidențelor incidentelor de securitate, inclusiv alertele de monitorizare;

50.7. fișele de control, monitorizare și audit;

50.8. copiile de siguranță și evidența politicilor de backup și restaurare;

50.9. fișierele de configurare operațională ale aplicației și mediului tehnologic;

50.10. nomenclatoarele, clasificatoarele, tabelele de coduri și regulile de validare utilizate în cadrul sistemului;

50.11. modelele de formulare, șabloanele și formatele de fișiere utilizate de sistem;

50.12. specificațiile tehnice de interoperabilitate, schemele de date și specificațiile de interfață utilizate pentru schimbul de date;

50.13. documentele tehnice privind administrarea rolurilor și profilurilor de acces;

50.14. documentele privind incidentele de securitate, măsurile de remediere și continuitatea funcționării sistemului.

Capitolul VII. Spațiul informațional al SI RIF

Secțiunea 1
Obiectele informaționale și identificatori ai obiectelor informaționale ale SI RIF

51. Spațiul informațional al SI RIF este constituit din totalitatea obiectelor informaționale, a atributelor, a metadatelor și a identificatorilor utilizați pentru formarea, evidența, prelucrarea, compararea, validarea, schimbul automatizat și utilizarea imaginilor faciale și a datelor de referință privind imaginile faciale.

52. Obiectele informaționale de bază ale SI RIF sunt:

52.1. imaginea facială identificată;

52.2. imaginea facială neidentificată;

52.3. datele de referință privind imaginea facială;

52.4. solicitarea de căutare automatizată a datelor de referință privind imaginile faciale;

52.5. răspunsul la solicitarea de căutare automatizată a datelor de referință privind imaginile faciale;

52.6. rezultatul comparării automatizate;

52.7. lista mostrelor pentru care există posibilitatea unei concordanțe;

52.8. înregistrarea privind confirmarea sau infirmarea concordanței;

52.9. metadatele aferente obiectelor informaționale gestionate în sistem.

53. Obiectele informaționale proprii ale SI RIF sunt obiectele prevăzute la pct. 52.1–52.9, care sunt create, gestionate și actualizate în cadrul SI RIF în scopurile prevăzute de prezentul Concept și de Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale.

54. În cadrul SI RIF pot fi utilizate, prin interoperabilitate, obiecte informaționale împrumutate din alte sisteme informaționale și resurse informaționale de stat, fără înregistrarea repetată a acestora în RIF, după cum urmează:

54.1. persoana fizică – din Registrul de stat al populației și/sau alte sisteme informaționale prevăzute de lege, identificată prin IDNP, iar în lipsa IDNP, prin alt identificator oficial disponibil în sistemul-sursă;

54.2. unitatea de drept, inclusiv autoritatea sau entitatea furnizoare/destinatară de date – din Registrul de stat al unităților de drept sau alte resurse informaționale prevăzute de lege, identificată prin IDNO, după caz;

54.3. cauza penală, dosarul de căutare, cazul individual sau alt obiect informațional conex – din sistemele informaționale ale autorităților competente, identificat prin identificatorul atribuit în sistemul-sursă;

54.4. datele aferente actelor de identitate, evidențelor criminalistice, dactiloscopice, genetice, de frontieră, migraționale sau altor evidențe relevante – din sistemele informaționale și resursele informaționale de stat prevăzute de cadrul normativ aplicabil, identificate prin identificatorii proprii ai sistemelor-sursă.

55. Obiectele informaționale împrumutate nu constituie obiecte primare de evidență ale RIF și nu se înregistrează repetat în RIF. SI RIF păstrează, după caz, numai identificatorii obiectelor împrumutate, datele minime necesare corelării, metadatele privind sursa datelor și informațiile necesare trasabilității accesării ori utilizării acestora. Datele aferente obiectelor informaționale împrumutate se consultă sau se consumă, după caz, prin mecanisme de interoperabilitate, în volumul minim necesar realizării scopului legal, fără constituirea în RIF a unei evidențe primare paralele a persoanelor, cauzelor, dosarelor ori altor obiecte informaționale deja înregistrate în sistemele-sursă.

56. Fiecare obiect informațional propriu gestionat în cadrul SI RIF este identificat în mod unic prin identificatori proprii ai SI RIF, iar obiectele informaționale împrumutate sunt identificate prin identificatorii atribuiți în sistemele informaționale sau resursele informaționale-sursă, cu respectarea interdicției de înregistrare repetată a obiectelor deja înregistrate în alte registre de stat.

57. Identificatorii principali utilizați în SI RIF sunt următorii:

57.1. pentru imaginea facială identificată – numărul de referință al imaginii faciale, identificatorul intern al înregistrării în SI RIF, precum și identificatorul persoanei fizice din sistemul-sursă, respectiv IDNP, după caz, sau alt identificator oficial atribuit în sistemul-sursă;

57.2. pentru imaginea facială neidentificată – numărul de referință al imaginii faciale, identificatorul intern al înregistrării în SI RIF, indicatorul caracterului neidentificat al imaginii faciale, precum și identificatorul cazului individual, al cauzei penale, al dosarului de căutare ori al altui obiect informațional conex din sistemul-sursă;

57.3. pentru datele de referință privind imaginea facială – numărul de referință și codurile asociate prevăzute de cadrul normativ aplicabil;

57.4. pentru solicitarea de căutare automatizată a datelor de referință privind imaginile faciale– numărul solicitării, data și ora solicitării, codul statului solicitant precum și, datele de referință privind imaginile faciale;

57.5. pentru răspunsul la solicitarea de căutare automatizată a datelor de referință privind imaginile faciale – numărul răspunsului, data și ora răspunsului, precum și numărul solicitării la care acesta se referă;

57.6. pentru rezultatul comparării automatizate – identificatorul rezultatului comparării, numărul de referință al imaginii faciale supuse comparării și, după caz, numărul de referință al mostrei comparative;

57.7. pentru înregistrarea privind confirmarea sau infirmarea concordanței – identificatorul validării, identificatorul rezultatului comparării și datele privind statutul validării.

57.8. pentru obiectele informaționale împrumutate – identificatorii atribuiți acestora în sistemele informaționale și resursele informaționale-sursă, inclusiv IDNP pentru persoana fizică, IDNO pentru unitatea de drept și identificatorul cauzei penale, dosarului de căutare, cazului individual ori al altui obiect informațional conex, după caz.

58. Identificatorii obiectelor informaționale sunt corelați cu procesele și funcțiile descrise în Capitolul IV „Spațiul funcțional al SI RIF”, ceea ce permite integrarea proceselor de evidență, comparare, validare, raportare, schimb automatizat și arhivare.

59. Identificatorii utilizați în SI RIF sunt aliniați la cerințele cadrului normativ național și, după caz, la standardele și cerințele tehnice internaționale aplicabile, astfel încât să fie asigurată interoperabilitatea cu alte sisteme informaționale de stat și cu infrastructurile externe utilizate în cooperarea polițienească internațională.

60. Structura identificatorilor proprii ai SI RIF, regulile de generare, utilizare, corelare și păstrare a acestora, precum și regulile de utilizare a identificatorilor obiectelor informaționale împrumutate se stabilesc prin Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale și prin documentația tehnică aferentă sistemului, cu respectarea cadrului normativ aplicabil registrelor de stat și interoperabilității.

Secțiunea 2
Atributele obiectelor informaționale ale SI RIF

61. Atributele obiectelor informaționale ale SI RIF includ:

61.1. date privind obiectul informațional „imagine facială identificată”:

61.1.1. numărul de referință;

61.1.2. identificatorul intern al înregistrării;

61.1.3. statutul imaginii faciale;

61.1.4. imaginea facială;

61.1.5. datele privind sursa imaginii faciale;

61.1.6. data și locul prelevării, captării sau extragerii imaginii faciale;

61.1.7. temeiul introducerii imaginii faciale în registru;

61.1.8. datele privind autoritatea sau entitatea care a introdus imaginea facială;

61.1.9. identificatorul persoanei fizice din sistemul-sursă, respectiv IDNP, după caz, sau alt identificator oficial atribuit în sistemul-sursă;

61.1.10. datele minime de identificare ale persoanei fizice, preluate sau verificate din sistemul-sursă, strict necesare pentru confirmarea concordanței, identificarea persoanei ori furnizarea informațiilor suplimentare în condițiile legii, fără constituirea unei evidențe primare a persoanelor în RIF;

61.1.11. datele privind cauza penală, dosarul de căutare sau alt obiect informațional conex, după caz;

61.1.12. datele privind rezultatul comparării automatizate, după caz;

61.1.13. datele privind confirmarea sau infirmarea concordanței, după caz;

61.1.14. datele privind actualizarea, rectificarea, completarea, blocarea, radierea sau arhivarea informației.

61.2. date privind obiectul informațional „imagine facială neidentificată”:

61.2.1. numărul de referință;

61.2.2. identificatorul intern al înregistrării;

61.2.3. statutul imaginii faciale;

61.2.4. indicatorul caracterului neidentificat al imaginii faciale;

61.2.5. imaginea facială;

61.2.6. datele privind sursa imaginii faciale;

61.2.7. data și locul prelevării, captării sau extragerii imaginii faciale;

61.2.8. temeiul introducerii imaginii faciale în registru;

61.2.9. datele privind autoritatea sau entitatea care a introdus imaginea facială;

61.2.10. identificatorul cauzei penale, dosarului de căutare, cazului individual sau al altui obiect informațional conex, atribuit în sistemul-sursă, după caz;

61.2.11. datele privind rezultatul comparării automatizate, după caz;

61.2.12. datele privind confirmarea sau infirmarea concordanței, după caz;

61.2.13. datele privind identificarea ulterioară a persoanei, după caz;

61.2.14. datele privind actualizarea, rectificarea, completarea, blocarea, radierea sau arhivarea informației.

61.3. date privind obiectul informațional „date de referință privind imaginea facială”:

61.3.1. imaginea facială;

61.3.2. numărul de referință;

61.3.3. codul statului care deține imaginea facială;

61.3.4. indicatorul care arată caracterul identificat sau neidentificat al imaginii faciale;

61.3.5. alte metadate strict necesare pentru compararea și schimbul automatizat, fără a permite identificarea directă a persoanei.

61.4. date privind obiectul informațional „solicitarea de căutare automatizată a datelor de referință privind imaginile faciale”:

61.4.1. codul statului solicitant;

61.4.2. data solicitării;

61.4.3. ora solicitării;

61.4.4. numărul solicitării;

61.4.5. datele de referință privind imaginea facială.

61.5. date privind obiectul informațional „răspunsul la solicitarea de căutare automatizată a datelor de referință privind imaginile faciale”:

61.5.1. mențiunea existenței unei concordanțe, a mai multor concordanțe sau a inexistenței concordanței;

61.5.2. data solicitării;

61.5.3. ora solicitării;

61.5.4. numărul solicitării;

61.5.5. data răspunsului;

61.5.6. ora răspunsului;

61.5.7. numărul răspunsului;

61.5.8. codul statului solicitant;

61.5.9. codul statului solicitat;

61.5.10. numerele de referință ale imaginilor faciale din statul solicitant și din statul solicitat;

61.5.11. imaginile faciale între care s-a stabilit o concordanță.

61.6. date privind obiectul informațional „rezultatul comparării automatizate”:

61.6.1. identificatorul rezultatului comparării;

61.6.2. numărul de referință al imaginii faciale supuse comparării;

61.6.3. numărul de referință al mostrei comparative, după caz;

61.6.4. data și ora comparării;

61.6.5. rezultatul comparării;

61.6.6. nivelul de asemănare, după caz;

61.6.7. datele privind componenta sau procesul tehnic prin care a fost generat rezultatul;

61.6.8. statutul rezultatului comparării.

61.7. date privind obiectul informațional „lista mostrelor pentru care există posibilitatea unei concordanțe”:

61.7.1. identificatorul listei;

61.7.2. identificatorul rezultatului comparării automatizate;

61.7.3. numărul de referință al imaginii faciale supuse comparării;

61.7.4. numerele de referință ale mostrelor comparative incluse în listă;

61.7.5. nivelul de asemănare aferent fiecărei mostre, după caz;

61.7.6. ordinea mostrelor în listă;

61.7.7. data și ora formării listei;

61.7.8. statutul listei.

61.8. date privind obiectul informațional „înregistrarea privind confirmarea sau infirmarea concordanței”:

61.8.1. identificatorul validării;

61.8.2. identificatorul rezultatului comparării;

61.8.3. data și ora validării;

61.8.4. rezultatul validării;

61.8.5. datele privind persoana calificată care a efectuat validarea;

61.8.6. observațiile privind confirmarea sau infirmarea concordanței, după caz.

61.9. date privind obiectul informațional „metadatele aferente obiectelor informaționale”:

61.9.1. sursa datelor;
61.9.2. data și ora recepționării;
61.9.3. temeiul legal al introducerii;
61.9.4. istoricul actualizărilor;
61.9.5. legătura cu alte obiecte informaționale;
61.9.6. informații privind jurnalizarea și trasabilitatea operațiunilor;
61.9.7. identificatorul obiectului informațional împrumutat și denumirea sistemului informațional sau a resursei informaționale-sursă din care acesta este preluat ori consultat, după caz.

62. Datele de referință privind imaginea facială puse la dispoziție prin intermediul SI RIF nu conțin date suplimentare care permit identificarea directă a persoanei.

63. Fiecare obiect informațional include atributul obligatoriu „statut", care indică starea curentă a acestuia, inclusiv, după caz, activ, actualizat, blocat, radiat, arhivat sau altă stare stabilită prin Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale.

64. Structura tehnică detaliată a atributelor obiectelor informaționale gestionate în SI RIF, precum și regulile tehnice de completare, validare, actualizare și corelare automată a acestora se stabilesc prin documentația tehnică aferentă sistemului.

Secțiunea 3
Nomenclatoarele, clasificatoarele și regulile de validare ale SI RIF

65. În cadrul SI RIF se utilizează nomenclatoare, clasificatoare, tabele de coduri și reguli de validare necesare asigurării exactității, coerenței, interoperabilității și calității datelor gestionate în sistem.

66. Nomenclatoarele și clasificatoarele utilizate în cadrul SI RIF includ, după caz:
66.1. clasificatorul autorităților și entităților participante;
66.2. clasificatorul categoriilor de utilizatori și al profilurilor de acces;
66.3. nomenclatorul tipurilor și surselor imaginilor faciale;
66.4. nomenclatorul statutelor imaginilor faciale și al obiectelor informaționale;
66.5. clasificatorul temeiurilor legale de introducere, actualizare, blocare, radiere și arhivare a datelor;
66.6. nomenclatorul tipurilor de obiecte informaționale gestionate în sistem;
66.7. nomenclatorul rezultatelor comparării automatizate;
66.8. nomenclatorul rezultatelor validării concordanței;
66.9. clasificatorul incidentelor de securitate și al măsurilor aplicate;
66.10. clasificatorul motivelor de rectificare, completare, actualizare, blocare, radiere și arhivare a datelor;
66.11. nomenclatorul canalelor și tipurilor de schimb de date;
66.12. clasificatorul codurilor de țară și al altor coduri utilizate în schimbul automatizat al datelor;
66.13. alte nomenclatoare, clasificatoare și tabele de coduri necesare funcționării sistemului.

67. Nomenclatoarele, clasificatoarele, tabelele de coduri și regulile de validare se aprobă de către deținătorul sistemului, potrivit competențelor stabilite prin actele normative aplicabile și prin actele administrative cu caracter normativ.

68. Nomenclatoarele și clasificatoarele utilizate în cadrul SI RIF sunt compatibile, după caz, cu nomenclatoarele și clasificatoarele utilizate în alte sisteme informaționale și resurse informaționale relevante ale statului, în vederea asigurării interoperabilității și schimbului de date.

69. Regulile de validare aplicabile datelor introduse și procesate în SI RIF asigură:
69.1. verificarea completitudinii datelor obligatorii;
69.2. verificarea corectitudinii formatului datelor;
69.3. verificarea unicității identificatorilor și a numerelor de referință;
69.4. verificarea coerenței logice dintre atributele obiectelor informaționale;

69.5. verificarea corelației dintre imaginea facială, datele de referință și metadatele aferente;

69.6. verificarea statutului obiectelor informaționale și a condițiilor de modificare a acestuia;

69.7. verificarea respectării temeiului legal pentru introducerea, actualizarea, blocarea, radierea sau arhivarea datelor;

69.8. verificarea calității minime a imaginii faciale pentru utilizarea acesteia în compararea automatizată;

69.9. verificarea corectitudinii datelor utilizate în solicitările și răspunsurile de căutare automatizată;

69.10. verificarea corectitudinii datelor schimbate prin interoperabilitate cu alte sisteme informaționale.

70. Introducerea și prelucrarea datelor în sistem se efectuează numai după validarea acestora conform regulilor stabilite pentru obiectul informațional respectiv.

71. În cazul constatării unor erori, neconcordanțe, lipsuri ori incompatibilități, sistemul permite respingerea, suspendarea procesării, marcarea distinctă sau returnarea datelor pentru completare ori rectificare, după caz.

72. Regulile de validare asigură prevenirea introducerii datelor incomplete, eronate, contradictorii, duplicative ori incompatibile cu structura și scopul SI RIF.

73. Structura și conținutul nomenclatoarelor, clasificatoarelor, tabelelor de coduri și regulilor de validare, precum și modul de administrare și actualizare a acestora se stabilesc prin documentația tehnică aferentă sistemului.

Secțiunea 4
Interacțiunea SI RIF cu alte sisteme informaționale și cu sistemele informaționale partajate

74. SI RIF este găzduit pe platforma tehnologică guvernamentală comună (MCloud) în conformitate cu Hotărârea Guvernului nr. 128/2014 cu privire la platforma tehnologică guvernamentală comună (MCloud), iar aspectele ce țin de găzduirea, administrarea tehnică a infrastructurii și securitatea cibernetică se coordonează cu Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, potrivit cadrului normativ aplicabil.

75. Pentru schimbul de date și interoperabilitatea cu alte sisteme informaționale și resurse informaționale de stat, SI RIF interacționează prin intermediul platformei guvernamentale de interoperabilitate (MConnect), inclusiv, după caz, cu utilizarea componentei MConnect Events prin interfețe de programare a aplicațiilor (API), pentru expunerea și consumul evenimentelor de sistem relevante pentru interoperabilitate, în condițiile cadrului normativ aplicabil, a cerințelor tehnice stabilite de Instituția publică „Agenția de Guvernare Electronică”, ale cerințelor de securitate și ale documentației tehnice aferente SI RIF, precum și cu următoarele sisteme informaționale partajate:

75.1. serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea utilizatorilor și controlul accesului în cadrul sistemului;

75.2. serviciul electronic guvernamental integrat de semnătură electronică (MSign) – pentru semnarea documentelor electronice, după caz;

75.3. serviciul electronic guvernamental de jurnalizare (MLog) – pentru asigurarea evidenței operațiunilor și a trasabilității activităților desfășurate în sistem;

75.4. serviciul guvernamental de notificare electronică (MNotify) – pentru notificarea furnizorilor de date, registratorilor și utilizatorilor, după caz.

76. SI RIF interacționează cu următoarele sisteme informaționale și resurse informaționale relevante ale statului:

76.1. Sistemul informațional automatizat „Registrul informației criminalistice și criminologice”;

76.2. Sistemul informațional automatizat „Registrul dactiloscopic”;

76.3. Sistemul informațional „Registrul de stat al populației”;

76.4. Sistemul informațional al Inspectoratului General al Poliției de Frontieră;

76.5. Sistemul informațional al Inspectoratului General pentru Migrație;

76.6. alte sisteme informaționale și resurse informaționale de stat, stabilite de cadrul normativ aplicabil.

77. Interacțiunea cu sistemele informaționale prevăzute la pct. 76 se realizează exclusiv în scopul formării, actualizării, verificării, utilizării și validării datelor gestionate prin SI RIF, precum și pentru asigurarea schimbului de date în condițiile legii. În cadrul acestei interacțiuni pot fi consumate sau furnizate, după caz și în limita necesității funcționale documentate, următoarele categorii de date:

77.1. imagini faciale și date de referință privind imaginile faciale, în cazurile prevăzute de lege;

77.2. metadate aferente imaginilor faciale, inclusiv sursa, data, temeiul și contextul obținerii acestora;

77.3. identificatori tehnici, numere de referință, coduri și date necesare corelării obiectelor informaționale;

77.4. date necesare verificării identității persoanei sau corelării cu cazul individual, cauza penală, dosarul de căutare ori alt obiect informațional relevant;

77.5. rezultate ale comparării automatizate, lista mostrelor pentru care există posibilitatea unei concordanțe și înregistrări privind confirmarea sau infirmarea concordanței;

77.6. date de jurnalizare, audit și trasabilitate, în limitele necesare verificării legalității accesului și schimbului de date.

78. Dacă, pentru introducerea, actualizarea ori utilizarea datelor în Registrul imaginilor faciale, legislația prevede deținerea unor date sau documente disponibile în resursele informaționale ale altor autorități publice, acestea pot fi consumate sau furnizate prin intermediul platformei de interoperabilitate (MConnect).

79. La nivel internațional, SI RIF contribuie la:

79.1. realizarea schimbului automatizat al datelor de referință privind imaginile faciale, în condițiile cadrului normativ aplicabil cooperării polițienești internaționale, ale tratatelor internaționale și ale actelor de punere în aplicare;

79.2. furnizarea, ulterior unei concordanțe confirmate, a datelor de bază și a informațiilor suplimentare, în condițiile cadrului normativ aplicabil cooperării polițienești internaționale, ale tratatelor internaționale și ale actelor de punere în aplicare;

79.3. interacțiunea cu infrastructurile și mecanismele externe utilizate în cooperarea polițienească internațională, în condițiile legii, tratatelor internaționale și ale actelor de punere în aplicare;

79.4. aplicarea măsurilor de securitate, confidențialitate și trasabilitate la transmiterea transfrontalieră a datelor.

80. Schimbul de date dintre SI RIF și alte sisteme informaționale se realizează conform următoarelor principii:

80.1. legalitate – schimbul de date se realizează numai în temeiul și în limitele legii;

80.2. securitate – datele sunt protejate împotriva accesului neautorizat și a altor riscuri de securitate;

80.3. trasabilitate – fiecare acces și transfer de date este înregistrat și poate fi verificat ulterior;

80.4. proporționalitate – se transmit numai datele necesare și relevante pentru scopul urmărit;

80.5. interoperabilitate – schimbul de date se realizează prin mecanisme compatibile juridic, organizatoric, semantic și tehnic;

80.6. reciprocitate – schimbul de date cu entitățile externe se realizează în condițiile prevăzute de tratatele internaționale, acordurile și aranjamentele aplicabile, încheiate potrivit legii.

81. Subiecții care participă la formarea și actualizarea Registrului imaginilor faciale prin consumul sau furnizarea de date prin interoperabilitate sunt autoritățile și entitățile publice care

dețin ori administrează sisteme informaționale și resurse informaționale relevante, în limitele competențelor prevăzute de lege.

82. La proiectarea și dezvoltarea interfețelor SI RIF se ține cont, în măsura aplicabilă, de modelul unitar de design prevăzut de Hotărârea Guvernului nr. 677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design.

83. Categoriile concrete de date consumate și furnizate, temeiurile juridice, condițiile de acces, rolurile participanților, interfețele utilizate, măsurile de securitate și regulile de jurnalizare se stabilesc prin Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale, prin actele normative aplicabile și prin documentația tehnică aferentă SI RIF.

Secțiunea 5
Scenariile de bază utilizate în SI RIF

84. Scenariile de bază utilizate în SI RIF descriu fluxurile funcționale și informaționale principale prin care se realizează alimentarea, administrarea, compararea, validarea, utilizarea și schimbul automatizat al imaginilor faciale și al datelor de referință privind imaginile faciale.

85. Scenariul de bază privind introducerea primară a datelor presupune:

85.1. recepționarea imaginilor faciale și a datelor conexe din surse autorizate;

85.2. verificarea formală și tehnică a datelor recepționate;

85.3. atribuirea numărului de referință;

85.4. clasificarea și marcarea distinctă a imaginilor faciale identificate și neidentificate;

85.5. înregistrarea datelor și a metadatelor aferente în Registrul imaginilor faciale.

86. Scenariul de bază privind actualizarea și administrarea datelor presupune:

86.1. actualizarea, rectificarea și completarea datelor introduse în sistem;

86.2. modificarea statutului obiectelor informaționale, după caz;

86.3. blocarea, radierea și arhivarea datelor;

86.4. păstrarea temeiului legal al operațiunii, a istoricului actualizărilor și, după caz, a datelor privind rezultatul comparării automatizate și confirmarea ori infirmarea concordanței.

87. Scenariul de bază privind formarea și utilizarea repozitoriului de date comparative privind imaginile faciale presupune:

87.1. colectarea și centralizarea mostrelor comparative din surse autorizate;

87.2. asocierea mostrelor comparative cu setul de metadate ori cu identificatorii necesari susținerii procesului de identificare;

87.3. actualizarea și utilizarea repozitoriului în procesul comparării automatizate.

88. Scenariul de bază privind compararea automatizată a datelor de referință privind imaginile faciale presupune:

88.1. inițierea unei solicitări de comparare în raport cu un caz individual;

88.2. contrapunerea automată a imaginii faciale cu mostrele comparative disponibile, inclusiv după algoritmul 1:1 și 1:N;

88.3. determinarea nivelului de asemănare, ca indicator tehnic utilizat pentru ordonarea și evaluarea preliminară a mostrelor comparative, fără ca acesta să producă prin sine efecte juridice, procesuale sau operaționale;

88.4. generarea rezultatului tehnic preliminar al comparării și, după caz, formarea listei mostrelor pentru care există posibilitatea unei concordanțe, listă care nu constituie concordanță confirmată până la validarea efectuată de personal calificat.

89. Scenariul de bază privind suportul identificării cazului sau persoanei presupune:

89.1. extragerea și formarea datelor de bază și a informațiilor suplimentare necesare identificării persoanei și, după caz, individualizării cazului;

89.2. corelarea imaginii faciale și a rezultatului comparării cu obiectele informaționale relevante din sistemele-sursă interoperabile;

89.3. furnizarea datelor necesare autorităților competente.

90. Scenariul de bază privind validarea concordanței presupune:

90.1. revizuirea manuală, de către personal calificat, a rezultatului comparării automatizate și, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe;

90.2. confirmarea sau infirmarea concordanței;

90.3. înregistrarea rezultatului validării și păstrarea acestuia în sistem.

91. Scenariul de bază privind căutarea și schimbul automatizat al datelor presupune:

91.1. formularea și transmiterea solicitării de căutare automatizată a datelor de referință privind imaginile faciale;

91.2. recepționarea și procesarea solicitării de căutare automatizată a datelor de referință privind imaginile faciale;

91.3. generarea și transmiterea răspunsului la solicitarea de căutare automatizată a datelor de referință privind imaginile faciale;

91.4. furnizarea, după caz, a datelor de bază și a informațiilor suplimentare ulterior unei concordanțe confirmate.

92. Scenariul de bază privind interoperabilitatea cu alte sisteme informaționale și cu sistemele informaționale partajate presupune:

92.1. consumul și furnizarea de date prin intermediul platformei de interoperabilitate (MConnect);

92.2. preluarea datelor și metadatelor din sistemele-sursă relevante;

92.3. utilizarea serviciilor guvernamentale partajate pentru autentificare, jurnalizare, semnare electronică, notificare și alte funcționalități necesare exploatării sistemului;

92.4. asigurarea trasabilității, securității și controlului accesului în procesul de schimb de date.

93. Scenariul de bază privind interacțiunea cu infrastructurile informaționale externe utilizate în cooperarea polițienească internațională presupune:

93.1. pregătirea și extragerea seturilor de date necesare;

93.2. transmiterea și recepționarea datelor în condițiile legii, ale tratatelor internaționale și ale actelor de punere în aplicare;

93.3. aplicarea măsurilor de confidențialitate, integritate, criptare, jurnalizare și protecție a datelor cu caracter personal;

93.4. utilizarea rezultatelor schimbului automatizat în condițiile legii.

94. Scenariul de bază privind administrarea, controlul și auditul sistemului presupune:

94.1. administrarea utilizatorilor, rolurilor și profilurilor de acces;

94.2. jurnalizarea operațiunilor efectuate în sistem;

94.3. monitorizarea și controlul utilizării sistemului;

94.4. gestionarea incidentelor de securitate;

94.5. auditarea și verificarea trasabilității operațiunilor.

Capitolul VIII. Structura informațională și tehnologică a SI RIF

95. Structura informațională și tehnologică a SI RIF reprezintă ansamblul resurselor informaționale, componentelor funcționale, mecanismelor de interoperabilitate, resurselor tehnice și aplicațiilor software utilizate pentru formarea, administrarea, utilizarea și schimbul automatizat al datelor de referință privind imaginile faciale.

96. Structura informațională a SI RIF include:

96.1. Registrul imaginilor faciale, ca resursă informațională departamentală de stat, specializată, ținută în formă electronică;

96.2. obiectele informaționale și atributele acestora;

96.3. datele de referință privind imaginile faciale;

96.4. metadatele aferente obiectelor informaționale;

96.5. nomenclatoarele, clasificatoarele, tabelele de coduri și regulile de validare;

96.6. evidențele privind solicitările și răspunsurile de căutare automatizată;

96.7. evidențele privind rezultatele comparării automatizate și validarea concordanței;

96.8. jurnalele operațiunilor și alte evidențe necesare asigurării trasabilității și controlului utilizării sistemului.

97. Structura tehnologică a SI RIF se bazează pe o arhitectură modulară, scalabilă, interoperabilă și securizată, care asigură separarea logică a componentelor de date, de procesare, de integrare, de administrare și de securitate.

98. Structura tehnologică a SI RIF include, cel puțin, următoarele componente:

98.1. componenta de stocare și administrare a datelor;

98.2. componenta de comparare biometrică facială;

98.3. componenta de suport al identificării cazului sau persoanei;

98.4. componenta de validare a concordanței;

98.5. componenta de interoperabilitate și schimb de date;

98.6. componenta de administrare a utilizatorilor, rolurilor și profilurilor de acces;

98.7. componenta de jurnalizare, monitorizare și audit;

98.8. componenta de securitate și protecție a datelor;

98.9. componenta de raportare și exploatare a datelor.

99. Componenta de stocare și administrare a datelor asigură evidența, păstrarea, actualizarea, rectificarea, completarea, blocarea, radierea și arhivarea obiectelor informaționale gestionate în cadrul sistemului.

100. Componenta de comparare biometrică facială asigură compararea automatizată a imaginilor faciale cu date comparative disponibile, inclusiv prin mecanisme de tip 1:1 și 1:N, și generarea rezultatului comparării.

101. Componenta de suport al identificării cazului sau persoanei asigură corelarea rezultatului comparării cu datele și metadatele relevante, inclusiv prin interacțiunea cu sistemele informaționale și resursele informaționale de stat interoperabile, în vederea identificării persoanei și, după caz, a individualizării cazului.

102. Componenta de validare a concordanței asigură verificarea rezultatului comparării automatizate de către personal calificat, precum și înregistrarea confirmării sau infirmării concordanței.

103. Componenta de interoperabilitate și schimb de date asigură interacțiunea SI RIF cu alte sisteme informaționale și resurse informaționale de stat, precum și, după caz, cu infrastructurile și mecanismele externe utilizate în cooperarea polițienească internațională, în condițiile legii, ale tratatelor internaționale și ale actelor de punere în aplicare.

104. Componenta de administrare a utilizatorilor, rolurilor și profilurilor de acces asigură gestionarea accesului autorizat și diferențiat la funcționalitățile și datele sistemului, în funcție de competențele stabilite de lege.

105. Componenta de jurnalizare, monitorizare și audit asigură evidența operațiunilor efectuate în sistem, trasabilitatea prelucrărilor, monitorizarea utilizării sistemului și suportul pentru controlul intern și audit.

106. Componenta de securitate și protecție a datelor asigură aplicarea măsurilor tehnice și organizatorice necesare pentru garantarea confidențialității, integrității, disponibilității, autenticității și rezilienței sistemului.

107. SI RIF utilizează, după caz, sisteme informaționale partajate și servicii guvernamentale comune pentru autentificare, semnare electronică, jurnalizare, notificare, schimb de date și găzduire, în condițiile cadrului normativ aplicabil.

108. Găzduirea și exploatarea tehnologică a SI RIF se realizează prin utilizarea platformei tehnologice guvernamentale comune, în conformitate cu cadrul normativ aplicabil și cu cerințele de securitate și continuitate a funcționării.

109. Schimbul de date și interoperabilitatea dintre SI RIF și alte sisteme informaționale se realizează, de regulă, prin intermediul platformei de interoperabilitate (MConnect), cu respectarea

cadrului normativ privind schimbul de date, interoperabilitatea, protecția datelor cu caracter personal și securitatea informației.

110.Structura informațională și tehnologică a SI RIF asigură:

110.1. integritatea și coerența datelor;

110.2. interoperabilitatea cu sistemele-sursă și cu sistemele informaționale partajate;

110.3. accesul autorizat și diferențiat;

110.4. jurnalizarea și trasabilitatea operațiunilor;

110.5. protecția datelor cu caracter personal și securitatea informației;

110.6. posibilitatea dezvoltării și extinderii ulterioare a sistemului.

111.Soluțiile tehnice utilizate în cadrul SI RIF permit implementarea funcționalităților prevăzute de cadrul normativ național și de actele Uniunii Europene relevante pentru căutarea și schimbul automatizat de date în scopul cooperării polițienești, în partea referitoare la imaginile faciale, inclusiv cerințele privind datele de referință, solicitările și răspunsurile automatizate și utilizarea în cazuri individuale prevăzute de Regulamentul (UE) 2024/982.

112.Structura detaliată a componentelor informaționale și tehnologice, cerințele funcționale și nefuncționale, mecanismele de integrare, modelele de date, protocoalele de schimb și condițiile de administrare tehnică se stabilesc prin documentația tehnică aferentă sistemului, iar măsurile generale de securitate se stabilesc prin Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale și prin actele normative aplicabile.

Capitolul IX. Asigurarea securității informaționale a SI RIF

113.Asigurarea securității informaționale a SI RIF include totalitatea măsurilor juridice, organizatorice, economice și tehnologice orientate spre prevenirea și diminuarea riscurilor de securitate aferente resurselor informaționale, componentelor funcționale și infrastructurii tehnologice ale sistemului.

114.Securitatea informațională presupune protecția SI RIF în toate etapele proceselor de colectare, recepționare, prelucrare, comparare, validare, stocare, utilizare și transmitere a datelor, împotriva acțiunilor accidentale sau intenționate, cu caracter artificial ori natural, care pot cauza prejudicii subiecților sistemului, datelor prelucrate și infrastructurii informaționale.

115.Asigurarea securității informaționale a SI RIF se realizează în conformitate cu legislația aplicabilă în domeniul securității cibernetice, protecției datelor cu caracter personal, securității informației, schimbului de date și interoperabilității, precum și cu actele normative care reglementează utilizarea serviciilor guvernamentale partajate și a infrastructurilor informaționale relevante.

116.Principalele pericole pentru securitatea informațională a SI RIF sunt:

116.1. colectarea, accesarea, copierea, utilizarea sau divulgarea ilegală a imaginilor faciale și a datelor de referință privind imaginile faciale;

116.2. compromiterea, perturbarea ori utilizarea neautorizată a proceselor și mecanismelor tehnologice de selectare, comparare, validare, prelucrare și schimb al datelor;

116.3. implementarea în produsele software a unor componente care realizează funcții neprevăzute în documentația tehnică;

116.4. elaborarea, distribuirea sau utilizarea programelor care afectează funcționarea normală a sistemului;

116.5. compromiterea mecanismelor de autentificare, autorizare și control al accesului;

116.6. scurgerea informației prin canale tehnice;

116.7. interceptarea informației în rețelele de transmitere a datelor și în liniile de comunicații, decodificarea acesteia ori impunerea informației false;

116.8. distrugerea, deteriorarea, alterarea, blocarea sau sustragerea suporturilor și resurselor informaționale;

116.9. utilizarea tehnologiilor, aplicațiilor sau mijloacelor de protecție necorespunzătoare ori necertificate, în măsura în care legea cere certificare;

116.10. încălcarea prevederilor legislației din domeniul protecției datelor cu caracter personal, securității informației și securității cibernetice;

116.11. accesul neautorizat la log-uri, rezultate ale comparării automatizate, înregistrări privind validarea concordanței ori alte date sensibile generate de sistem.

117.SI RIF asigură următoarele obiective de securitate:

117.1. autentificarea – garantează că zonele restricționate ale sistemului sunt accesibile numai utilizatorilor autorizați, cu identitate verificată, inclusiv prin utilizarea serviciului electronic guvernamental de autentificare și control al accesului (MPass), după caz;

117.2. confidențialitatea – garantează că imaginile faciale, datele de referință și celelalte date gestionate în sistem nu pot fi accesate de persoane neautorizate;

117.3. integritatea – garantează că datele gestionate în sistem nu sunt modificate, alterate ori distruse neautorizat;

117.4. disponibilitatea – garantează că datele și funcționalitățile sistemului sunt accesibile utilizatorilor autorizați atunci când este necesar;

117.5. nerepudierea – garantează că operațiunile efectuate în sistem nu pot fi negate ulterior de către autorii lor;

117.6. trasabilitatea – garantează că fiecare accesare și fiecare operațiune relevantă efectuată în sistem poate fi urmărită și verificată ulterior.

118.Pentru asigurarea unui nivel adecvat al securității informaționale a SI RIF, deținătorul și administratorul tehnic al sistemului elaborează și implementează politica de securitate informațională, care stabilește măsurile de securitate, rolurile, drepturile și obligațiile subiecților sistemului, procedurile de control al accesului, jurnalizare, răspuns la incidente, continuitate și recuperare.

119.Un element esențial al securității informaționale îl constituie păstrarea înregistrărilor de audit necesare pentru analiza integrității sistemului, monitorizarea utilizării acestuia și verificarea legalității operațiunilor efectuate. SI RIF utilizează mecanisme de audit intern, precum și serviciul electronic guvernamental de jurnalizare (MLog), în vederea asigurării evidenței operațiunilor și a trasabilității activităților desfășurate în sistem.

120.Pentru asigurarea interoperabilității și a schimbului de date cu alte sisteme și resurse informaționale de stat, activele semantice utilizate în SI RIF se înregistrează și se utilizează prin raportare la Sistemul informațional „Catalogul semantic”, aprobat prin Hotărârea Guvernului nr. 323/2021.

Capitolul X. Încheiere

121.Prezentul Concept descrie principalele aspecte organizaționale, metodologice, funcționale, informaționale și tehnologice în conformitate cu care este conceput și urmează a fi implementat SI RIF, ca soluție informațională specializată, destinată asigurării suportului informațional necesar autorităților competente în procesele de colectare, evidență, comparare, validare, utilizare și schimb automatizat al datelor de referință privind imaginile faciale.

122.Prin prezentul Concept este stabilit cadrul general de creare, dezvoltare și funcționare a SI RIF, precum și locul acestuia în arhitectura guvernării electronice și în spațiul informațional al statului. Soluția propusă corespunde necesităților funcționale ale autorităților competente, cerințelor de interoperabilitate, protecției datelor cu caracter personal, securității informaționale și nivelului actual de dezvoltare a infrastructurii digitale a Republicii Moldova.

123.Implementarea SI RIF va permite dezvoltarea unei resurse informaționale specializate, centralizate și interoperabile, necesare autorităților competente și altor instituții abilitate prin lege. Aceasta va oferi posibilitatea:

123.1. de a asigura o evidență unică, structurată și fiabilă a imaginilor faciale și a datelor de referință privind imaginile faciale;

123.2. de a consolida capacitățile autorităților competente în domeniul prevenirii, constatării și investigării infracțiunilor, al identificării persoanelor și al cooperării polițienești internaționale;

123.3. de a asigura compararea automatizată a imaginilor faciale, validarea concordanțelor și furnizarea, în condițiile legii, a datelor de bază și a informațiilor suplimentare;

123.4. de a crește nivelul de interoperabilitate cu alte sisteme informaționale și resurse informaționale relevante ale statului;

123.5. de a contribui la realizarea schimbului automatizat de date în condiții de legalitate, securitate, trasabilitate și protecție a datelor cu caracter personal;

123.6. de a crea premisele tehnice și organizatorice necesare alinierii progresive la cerințele europene aplicabile în domeniul căutării și schimbului automatizat de date în scopul cooperării polițienești, în partea referitoare la imaginile faciale.

Anexa nr. 2
aprobată prin Hotărârea Guvernului
nr._____/2026

REGULAMENT
privind modalitatea de ținere a Registrului imaginilor faciale

Capitolul I. Dispoziții generale

1. Prezentul Regulament stabilește modul de organizare, ținere, administrare, actualizare, utilizare, furnizare, protecție și arhivare a datelor din Registrul imaginilor faciale, ținut prin intermediul Sistemului informațional „Registrul imaginilor faciale” (în continuare – SI RIF), în vederea asigurării funcționării registrului ca resursă informațională departamentală de stat, specializată, destinată prelucrării imaginilor faciale, identificării biometrice faciale, validării concordanțelor și schimbului automatizat al datelor de referință privind imaginile faciale.

2. Regulamentul stabilește drepturile și obligațiile subiecților raporturilor juridice aferente ținerii RIF, categoriile de date gestionate, modalitatea de introducere, actualizare, rectificare, completare, blocare, radiere, arhivare și utilizare a datelor, regimul de acces la date, procedura de interoperabilitate și schimb de date, regulile privind compararea automatizată, validarea concordanței și evidența rezultatelor, precum și măsurile de securitate, jurnalizare, monitorizare, control și audit.

3. Prezentul Regulament se aplică autorităților publice, instituțiilor, entităților și persoanelor care, potrivit legii, au atribuții în procesul de formare, administrare, actualizare, utilizare, validare, furnizare sau schimb al datelor gestionate prin SI RIF, în măsura în care acestea furnizează, prelucrează, validează ori utilizează date din Registrul imaginilor faciale.

4. Registrul imaginilor faciale (în continuare – RIF) constituie resursă informațională departamentală de stat, specializată, ținută prin intermediul SI RIF, interoperabilă cu alte sisteme informaționale și resurse informaționale relevante ale statului, fără a substitui funcțiile de evidență primară ale acestora.

5. RIF se ține și se administrează în conformitate cu legislația privind informatizarea și resursele informaționale de stat, registrele, schimbul de date și interoperabilitatea, protecția datelor cu caracter personal, securitatea informației, securitatea cibernetică, precum și, după caz, cu actele normative și tratatele internaționale aplicabile cooperării polițienești internaționale.

6. Termenii și noțiunile utilizate în prezentul Regulament au semnificația prevăzută de legislația privind informatizarea și resursele informaționale de stat, cu privire la registrele de stat, schimbul de date și interoperabilitatea, protecția datelor cu caracter personal, securitatea cibernetică, de actele normative și tratatele internaționale aplicabile cooperării polițienești internaționale, precum și de Conceptul Sistemului informațional „Registrul imaginilor faciale”.

7. RIF se ține în limba română, în format electronic.

8. Orice operațiune de introducere, actualizare, rectificare, completare, consultare, extragere, comparare, validare, transmitere, blocare, radiere sau arhivare a datelor din RIF se efectuează exclusiv în condițiile legii, în limita competențelor atribuite, cu asigurarea jurnalizării și trasabilității operațiunii efectuate, precum și a posibilității verificării și auditului utilizării datelor.

Capitolul II. Subiecții raporturilor juridice în domeniul creării, exploatării și utilizării RIF

9. Funcțiile de bază privind crearea, exploatarea și utilizarea RIF sunt distribuite între următorii subiecți:

9.1. proprietarul sistemului;

9.2. posesorul sistemului;

9.3. deținătorul sistemului;

9.4. administratorul tehnic;

9.5. utilizatorii sistemului;
9.6. registratorii;
9.7. furnizorii de date;
9.8. destinatarii datelor.

10. Proprietarul RIF este statul, care își realizează dreptul de proprietate, gestionare și utilizare a datelor din acesta, în condițiile legii.

11. Posesor al RIF este Ministerul Afacerilor Interne, care asigură guvernanța instituțională a sistemului, coordonarea dezvoltării și utilizării acestuia, cooperarea dintre autoritățile participante, precum și, în condițiile legii, coordonarea instituțională a participării SI RIF la mecanismul de căutare și schimb automatizat transfrontalier al datelor de referință privind imaginile faciale.

12. Deținător al RIF este Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne, care asigură crearea, dezvoltarea, mentenanța aplicativă, funcționarea tehnică a aplicației, administrarea componentelor software, a bazelor de date, a interfețelor și a mecanismelor aplicative de securitate, jurnalizare, monitorizare și audit, precum și suportul tehnic necesar funcționării SI RIF, în limitele competențelor sale și în coordonare cu administratorul tehnic pentru aspectele ce țin de găzduire și infrastructura tehnologiilor informaționale, inclusiv a măsurilor necesare pentru asigurarea confidențialității, integrității, disponibilității și trasabilității schimbului automatizat transfrontalier de date.

13. Administrator tehnic al RIF este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, care, în limitele competențelor stabilite, asigură administrarea tehnică a infrastructurii tehnologiilor informaționale aferente găzduirii SI RIF, mentenanța infrastructurii gestionate, măsurile de securitate cibernetică și suportul tehnic aferent serviciilor prestate, fără a interveni în administrarea funcțională a datelor gestionate prin RIF.

14. Utilizatorii RIF sunt persoane fizice desemnate de către registratori, furnizorii de date și destinatarii datelor, care au acces autorizat la sistem în baza unui rol specific atribuit, conform politicilor de securitate și control al accesului, în limitele competențelor legale și numai pentru scopurile prevăzute de lege.

15. Registratorii sunt persoane autorizate, desemnate în condițiile legii, care efectuează în RIF operațiuni de introducere, actualizare, rectificare, completare, blocare, radiere și arhivare a datelor, inclusiv marcarea imaginilor faciale neidentificate, atribuirea, verificarea și menținerea evidenței numerelor de referință, actualizarea metadatelor aferente, înregistrarea solicitărilor și răspunsurilor de căutare automatizată, consemnarea rezultatelor comparării automatizate și a confirmării ori infirmării concordanței, precum și actualizarea datelor relevante pentru componenta de schimb automatizat transfrontalier, în limitele competențelor stabilite de lege și numai pentru scopurile prevăzute de cadrul normativ aplicabil.

16. În calitate de registratori ai RIF sunt desemnate persoane din cadrul următoarelor autorități și instituții, în limitele competențelor stabilite de lege:

16.1 subdiviziunile specializate ale Inspectoratului General al Poliției;
16.2 subdiviziunile specializate ale Inspectoratului General al Poliției de Frontieră;
16.3 subdiviziunile specializate ale Inspectoratului General pentru Migrație;
16.4 alte autorități și instituții abilitate prin lege, în măsura în care cadrul normativ special le conferă competența de a introduce, actualiza sau rectifica date în RIF.

17. Registratorii desemnați pentru componenta de schimb automatizat transfrontalier operează numai în cazuri individuale, cu utilizarea numerelor de referință, cu respectarea cerințelor de validare, jurnalizare și trasabilitate, precum și a procedurilor privind solicitările și răspunsurile de căutare automatizată, în condițiile legii.

18. Furnizorii de date sunt autoritățile și entitățile care furnizează, în condițiile legii, date, imagini faciale, metadate ori alte informații necesare formării, completării și actualizării Registrului imaginilor faciale, inclusiv prin mecanisme de interoperabilitate, precum și, după caz, pentru constituirea și actualizarea setului de date de referință destinat schimbului automatizat

transfrontalier, cu asigurarea legalității furnizării, exactității, actualității, relevanței, integrității și, după caz, a calității suficiente a imaginilor faciale pentru compararea automatizată.

19. În calitate de furnizori de date ai SI RIF sunt desemnate:

19.1. subdiviziunile specializate ale Inspectoratului General al Poliției;

19.2. subdiviziunile specializate ale Inspectoratului General al Poliției de Frontieră;

19.3. subdiviziunile specializate ale Inspectoratului General pentru Migrație;

19.4. Agenția Servicii Publice;

19.5. Serviciul de Informații și Securitate;

19.6. Administrația Națională a Penitenciarelor;

19.7. Inspectoratul Național de Probațiune;

19.8. alte autorități și entități, numai dacă furnizarea datelor este prevăzută expres de lege sau rezultă nemijlocit din atribuțiile stabilite prin lege.

20. Destinatarii datelor sunt autoritățile și entitățile care au dreptul legal de a accesa sau primi date din SI RIF pentru realizarea atribuțiilor ce le revin, în condițiile legii, inclusiv, după caz, pentru extragerea și furnizarea datelor de bază și a informațiilor suplimentare aferente unei concordanțe confirmate, prin canalele, procedurile și punctele de contact stabilite de cadrul normativ aplicabil schimbului automatizat transfrontalier de date, cu respectarea principiului accesului autorizat și diferențiat, a necesității funcționale, a jurnalizării și trasabilității operațiunilor, precum și a interdicției utilizării datelor pentru interogări generale, exploratorii sau în alte scopuri decât cele prevăzute de lege.

21. În calitate de destinatari ai datelor din RIF sunt desemnate autoritățile și entitățile care, potrivit legii, au competența de a accesa sau primi datele respective, exclusiv în volumul necesar exercitării atribuțiilor legale și cu respectarea profilurilor de acces aprobate:

21.1. subdiviziunile specializate ale Inspectoratului General al Poliției;

21.2. subdiviziunile specializate ale Inspectoratului General al Poliției de Frontieră;

21.3. subdiviziunile specializate ale Inspectoratului General pentru Migrație;

21.4. Agenția Servicii Publice, în limitele competențelor prevăzute de lege;

21.5. Serviciul de Informații și Securitate, în limitele competențelor prevăzute de lege;

21.6. Administrația Națională a Penitenciarelor, în limitele competențelor prevăzute de lege;

21.7. Inspectoratul Național de Probațiune, în limitele competențelor prevăzute de lege;

21.8. autoritățile și entitățile externe, în condițiile cadrului normativ aplicabil cooperării polițienești internaționale, ale tratatelor internaționale și ale actelor de punere în aplicare;

21.9. alte autorități publice competente, în condițiile legii.

22. Delimitarea competențelor dintre subiecții RIF, inclusiv cu celelalte resurse informaționale și cu infrastructurile și mecanismele externe utilizate în cooperarea polițienească internațională, se stabilește în mod expres prin prezentul Regulament, prin actele normative din domeniu și prin actele administrative emise în temeiul acestora.

Capitolul III. Drepturile și obligaţiile subiecţilor la crearea, exploatarea şi utilizarea RIF

Secțiunea 1
Drepturile și obligațiile posesorului RIF

23. Posesorul RIF este Ministerul Afacerilor Interne, care exercită următoarele drepturi:

23.1. să stabilească cerințele funcționale, organizaționale și de securitate aplicabile RIF;

23.2. să aprobe regulile interne privind administrarea accesului, rolurile și profilurile de acces ale utilizatorilor;

23.3. să solicite deținătorului, registratorilor, furnizorilor de date și destinatarilor datelor măsurile necesare pentru funcționarea legală și sigură a RIF;

23.4. să inițieze măsuri de dezvoltare, modernizare și interoperabilitate a RIF;

23.5. să coordoneze instituțional participarea RIF la mecanismul de căutare și schimb automatizat transfrontalier al datelor de referință privind imaginile faciale.

24. Posesorul SI RIF are obligația:

24.1. să asigure condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea RIF;

24.2. să organizeze și să coordoneze activitatea subiecților RIF în limita competențelor stabilite de lege;

24.3. să aprobe procedurile interne privind utilizarea RIF, administrarea accesului, validarea concordanțelor, jurnalizarea și auditul;

24.4. să asigure utilizarea RIF și a componentei de schimb automatizat transfrontalier numai în scopurile și în condițiile prevăzute de lege;

24.5. să asigure, prin intermediul mecanismelor prevăzute de lege, notificarea și actualizarea informațiilor privind conținutul bazei de date naționale privind imaginile faciale, condițiile tehnice și juridice ale căutărilor automatizate, lista autorităților autorizate și profilurile de acces ale personalului autorizat;

24.6. să monitorizeze implementarea și funcționarea RIF, inclusiv pe componenta de schimb automatizat transfrontalier;

24.7. să dispună măsuri de remediere în cazul deficiențelor, incidentelor de securitate sau utilizărilor neconforme ale RIF;

24.8. să asigure cooperarea interinstituțională necesară funcționării RIF și interoperabilității cu alte sisteme și resurse informaționale relevante.

Secțiunea 2
Drepturile și obligațiile deținătorului RIF

25. Deținătorul RIF este Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne, care dispune de următoarele drepturi:

25.1. să administreze și să exploateze tehnic RIF, în limitele competențelor stabilite de lege și ale sarcinilor atribuite de posesor;

25.2. să solicite subiecților RIF respectarea cerințelor tehnice și de securitate necesare funcționării sistemului;

25.3. să suspende sau să restricționeze, după caz, accesul tehnic la RIF în situații de incident de securitate, neconformitate sau risc iminent, cu informarea imediată a posesorului;

25.4. să efectueze lucrări de mentenanță, actualizare, restabilire și dezvoltare a RIF.

26. Deținătorul RIF are obligația:

26.1. să asigure crearea, funcționarea tehnică, mentenanța și dezvoltarea continuă a RIF;

26.2. să administreze componentele aplicative ale RIF, bazele de date, interfețele și componentele de interoperabilitate aflate în responsabilitatea sa, precum și să asigure administrarea tehnică aplicativă a sistemului, în coordonare cu administratorul tehnic pentru aspectele ce țin de infrastructura tehnologiilor informaționale și găzduire;

26.3. să administreze conturile de utilizator, drepturile și profilurile de acces, în baza actelor justificative și a deciziilor aprobate de posesor;

26.4. să asigure jurnalizarea, monitorizarea și trasabilitatea operațiunilor efectuate în RIF și păstrarea înregistrărilor de audit;

26.5. să implementeze măsurile tehnice și organizatorice necesare pentru asigurarea confidențialității, integrității, disponibilității, autenticității și trasabilității datelor;

26.6. să asigure, în condițiile legii și în limitele competențelor sale, funcționarea tehnică a componentei de schimb automatizat transfrontalier, inclusiv conectarea și integrarea tehnică a infrastructurii naționale relevante cu mecanismele și infrastructurile externe utilizate în cooperarea polițienească internațională;

26.7. să asigure implementarea tehnică a accesului personalului autorizat la infrastructurile utilizate pentru schimbul automatizat de date, în baza deciziilor și profilurilor aprobate de posesor ori de autoritatea competentă, inclusiv autentificarea, trasabilitatea accesărilor și actualizarea tehnică a profilurilor de acces;

26.8. să asigure copii de rezervă, continuitatea funcționării și recuperarea în caz de incident;

26.9. să informeze fără întârziere posesorul despre incidentele de securitate și disfuncționalitățile tehnice;

26.10. să asigure suportul tehnic și metodologic necesar subiecților RIF.

Secțiunea 3
Drepturile și obligațiile administratorului tehnic al RIF

27. Administratorul tehnic al RIF este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, care dispune de următoarele drepturi:

27.1. să solicite posesorului și deținătorului informațiile tehnice necesare pentru asigurarea găzduirii, administrării infrastructurii și securității cibernetice aferente SI RIF;

27.2. să propună măsuri tehnice necesare pentru asigurarea disponibilității, continuității, rezilienței și securității infrastructurii aferente SI RIF;

27.3. să informeze posesorul și deținătorul despre riscurile, vulnerabilitățile, incidentele sau neconformitățile tehnice identificate în aria sa de responsabilitate.

28. Administratorul tehnic al RIF are obligația:

28.1. să asigure, în limitele competențelor sale, administrarea tehnică a infrastructurii TI aferente găzduirii SI RIF;

28.2. să asigure mentenanța infrastructurii gestionate și suportul tehnic aferent serviciilor prestate;

28.3. să aplice măsurile de securitate cibernetică ce țin de infrastructura administrată;

28.4. să asigure continuitatea și disponibilitatea infrastructurii gestionate, potrivit nivelurilor de servicii stabilite;

28.5. să coopereze cu posesorul și deținătorul RIF în procesul de gestionare a incidentelor de securitate și de restabilire a funcționării sistemului;

28.6. să respecte regimul de confidențialitate, securitate și acces autorizat aplicabil datelor și infrastructurii SI RIF.

29. Administratorul tehnic nu exercită atribuții de registrator, furnizor de date sau destinatar al datelor și nu intervine în administrarea funcțională a imaginilor faciale, a datelor de referință privind imaginile faciale ori a rezultatelor comparării automatizate, cu excepția accesului tehnic strict necesar pentru realizarea atribuțiilor sale, în condițiile legii, cu jurnalizarea operațiunilor efectuate.

Secțiunea 4
Drepturile și obligațiile registratorilor RIF

30. Registratorii RIF sunt persoanele autorizate din cadrul Inspectoratului General al Poliției și, după caz, din alte autorități competente, desemnate de posesorul sistemului.

31. Registratorii au dreptul:

31.1. să introducă, actualizeze, rectifice, completeze, blocheze, radieze și arhiveze date în RIF, în limitele rolului și profilului de acces atribuit;

31.2. să atribuie, să verifice și să gestioneze numerele de referință pentru imaginile faciale introduse în RIF;

31.3. să consulte și să utilizeze datele necesare realizării operațiunilor de registratură și actualizare a RIF;

31.4. să inițieze, în cazurile prevăzute de lege, solicitări de comparare automatizată și să înregistreze rezultatele aferente;

31.5. să solicite furnizorilor de date clarificarea, completarea ori corectarea datelor furnizate.

32. Registratorii au obligația:

32.1. să efectueze operațiuni în RIF numai în temeiul legii, în limita atribuțiilor de serviciu și exclusiv pentru scopurile prevăzute de cadrul normativ aplicabil;

32.2. să asigure introducerea, actualizarea și rectificarea datelor în mod complet, exact, actual și la timp;

32.3. să verifice temeiul legal al operațiunii, existența documentelor și informațiilor justificative, precum și coerența datelor introduse;

32.4. să marcheze distinct imaginile faciale neidentificate și să asigure menținerea separată a datelor relevante pentru componenta de schimb automatizat transfrontalier;

32.5. să atribuie și să mențină corect evidența numerelor de referință;

32.6. să înregistreze solicitările și răspunsurile de căutare automatizată, rezultatele comparării automatizate și, după caz, confirmarea sau infirmarea concordanței;

32.7. să opereze pe componenta de schimb automatizat transfrontalier numai în cazuri individuale, cu respectarea procedurilor privind validarea, jurnalizarea și trasabilitatea;

32.8. să asigure confidențialitatea și protecția datelor cu caracter personal la care are acces;

32.9. să informeze fără întârziere deținătorul și conducătorul ierarhic despre erorile constatate, accesările neautorizate, incidentele de securitate sau alte neconformități.

Secțiunea 5
Drepturile și obligațiile furnizorului de date ai RIF

33. Furnizorii de date RIF sunt instituțiile publice și persoanele juridice de drept public sau privat care, în baza competențelor legale, transmit date, imagini faciale, metadate ori alte informații necesare formării, completării și actualizării RIF, inclusiv prin mecanisme de interoperabilitate, precum și, după caz, pentru constituirea și actualizarea setului de date de referință destinat schimbului automatizat transfrontalier.

34. Furnizorii de date au dreptul:

34.1. să furnizeze date, imagini faciale, metadate și alte informații relevante în RIF, în limitele competențelor stabilite de lege;

34.2. să solicite rectificarea ori actualizarea datelor furnizate anterior, atunci când constată inexactități, neactualitate sau lipsa relevanței acestora;

34.3. să utilizeze mecanismele de interoperabilitate și canalele autorizate pentru furnizarea datelor, în condițiile legii;

34.4. să fie informați despre neconcordanțele sau deficiențele identificate în datele furnizate de ei.

35. Furnizorii de date au obligația:

35.1. să furnizeze date, imagini faciale, metadate și alte informații relevante obținute din surse autorizate și numai în condițiile legii;

35.2. să asigure legalitatea furnizării, exactitatea, actualitatea, relevanța, integritatea și, după caz, calitatea suficientă a imaginilor faciale pentru compararea automatizată;

35.3. să furnizeze, după caz, datele necesare constituirii și actualizării setului de date de referință destinat schimbului automatizat transfrontalier;

35.4. să respecte cerințele privind separarea categoriilor de date, marcarea imaginilor faciale neidentificate și limitarea datelor puse la dispoziție pentru căutare automatizată;

35.5. să utilizeze numai mecanismele de interoperabilitate și canalele autorizate pentru furnizarea datelor;

35.6. să comunice fără întârziere rectificările, actualizările sau retragerile necesare, dacă datele furnizate s-au dovedit inexacte, neactuale ori furnizate fără temei legal;

35.7. să respecte cerințele privind protecția datelor cu caracter personal, securitatea informației, securitatea cibernetică, jurnalizarea și trasabilitatea operațiunilor efectuate.

Secțiunea 6
Drepturile și obligațiile destinatarilor datelor din RIF

36. Destinatarii datelor din RIF sunt autorități publice, instituții și alte persoane juridice care au competența de a accesa și utiliza datele conținute în registru, pentru realizarea atribuțiilor legale, inclusiv, după caz, pentru extragerea și furnizarea datelor de bază și a informațiilor suplimentare aferente unei concordanțe confirmate, prin canalele, procedurile și punctele de contact stabilite de cadrul normativ aplicabil schimbului automatizat transfrontalier de date.

37. Destinatarii datelor au dreptul:

37.1. să acceseze sau să primească date din RIF numai în măsura necesară exercitării atribuțiilor ce le revin și în limitele profilurilor de acces aprobate;

37.2. să utilizeze datele primite pentru prevenirea, depistarea, constatarea și investigarea infracțiunilor, identificarea ori verificarea identității persoanelor, căutarea persoanelor dispărute, identificarea cadavrelor ori a părților acestora și alte scopuri prevăzute de lege;

37.3. să solicite, după caz, extragerea și furnizarea datelor de bază și a informațiilor suplimentare aferente unei concordanțe confirmate, prin canalele, procedurile și punctele de contact stabilite de cadrul normativ aplicabil;

37.4. să solicite verificarea, rectificarea sau actualizarea datelor atunci când constată neconcordanțe.

38. Destinatarii datelor au obligația:

38.1. să acceseze și să utilizeze datele numai în scopurile și în limitele prevăzute de lege;

38.2. să respecte regimul diferențiat de acces, în funcție de categoria datelor, temeiul legal al solicitării și scopul utilizării acestora;

38.3. să nu utilizeze datele pentru interogări generale, exploratorii ori pentru alte scopuri decât cele prevăzute de lege;

38.4. să utilizeze datele de referință privind imaginile faciale și, după caz, să solicite extragerea datelor de bază și a informațiilor suplimentare numai ulterior unei concordanțe confirmate;

38.5. să utilizeze componenta de schimb automatizat transfrontalier numai prin canalele, procedurile și punctele de contact stabilite de cadrul normativ aplicabil;

38.6. să respecte cerințele privind confidențialitatea, integritatea, disponibilitatea, jurnalizarea și trasabilitatea operațiunilor efectuate;

38.7. să nu transmită, să nu divulge și să nu pună la dispoziția terților datele obținute din RIF, cu excepția cazurilor expres prevăzute de lege, de tratatele internaționale aplicabile sau de actele de punere în aplicare, cu respectarea condițiilor stabilite de autoritatea competentă furnizoare;

38.8. să informeze fără întârziere furnizorul sau registratorul competent atunci când constată că datele primite sunt inexacte, neactuale sau au fost transmise cu încălcarea legii.

Capitolul IV. Ținerea și asigurarea funcționării RIF

Secțiunea 1

Dispoziții generale privind ținerea RIF

39. Registrul imaginilor faciale se ține în formă electronică, prin intermediul SI RIF, în condițiile prezentului Regulament, ale actelor normative speciale aplicabile și ale tratatelor internaționale la care Republica Moldova este parte, după caz.

40. Ținerea RIF presupune totalitatea operațiunilor de recepționare, verificare, introducere, înregistrare, actualizare, rectificare, completare, blocare, radiere, arhivare, consultare, extragere, comparare, validare și furnizare a datelor, efectuate în limitele competențelor legale și ale profilurilor de acces aprobate.

41. Operațiunile asupra datelor din RIF se efectuează numai de către utilizatori autorizați, pe baza rolurilor atribuite, în condițiile respectării principiilor legalității, necesității, proporționalității, exactității, limitării scopului, securității informației și trasabilității.

42. Datele din RIF se gestionează distinct, după caz, în cadrul:

42.1. componentei naționale a registrului;

42.2. setului de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier, constituit și utilizat exclusiv în condițiile legii.

43. În RIF se introduc și se gestionează distinct imaginile faciale identificate și imaginile faciale neidentificate. Fiecare imagine facială introdusă în registru este însoțită de metadatele aferente și de numărul de referință atribuit potrivit regulilor stabilite de prezentul Regulament.

44. În RIF se introduc și se gestionează, în condițiile legii și ale prezentului Regulament, informații privind rezultatele comparării automatizate, informații privind confirmarea sau

infirmarea concordanței, evidențe privind solicitările și răspunsurile de căutare automatizată, jurnalele operațiunilor și alte evidențe necesare asigurării trasabilității și controlului utilizării datelor.

45. Orice operațiune asupra datelor din RIF trebuie să fie justificată prin scopul legal urmărit, să se întemeieze pe documente, date sau informații provenite din surse autorizate și să fie limitată la datele strict necesare realizării acestui scop.

Secțiunea a 2-a
Introducerea și înregistrarea datelor în RIF

46. Introducerea datelor în RIF se efectuează de către registratori, în temeiul documentelor justificative, al datelor furnizate de autoritățile competente, al informațiilor obținute prin interoperabilitate, al rezultatelor activităților de constatare tehnico-științifică sau expertiză judiciară, precum și al altor surse autorizate de lege.

47. Înainte de introducerea datelor în RIF, registratorul verifică:

47.1. competența legală pentru efectuarea operațiunii;

47.2. existența temeiului juridic și a documentului justificativ;

47.3. caracterul necesar, relevant și neexcesiv al datelor;

47.4. exactitatea, completitudinea și actualitatea datelor disponibile;

47.5. calitatea suficientă a imaginii faciale pentru prelucrarea ulterioară, inclusiv pentru compararea automatizată, după caz;

47.6. inexistența unor dublări vădite sau, dacă acestea există, necesitatea tratării lor potrivit regulilor de consolidare a evidenței.

48. În cazul în care la momentul recepționării nu sunt disponibile toate datele necesare, registratorul poate efectua o înregistrare inițială, cu marcarea caracterului incomplet al acesteia și cu completarea ulterioară a datelor, imediat ce acestea devin disponibile în mod legal.

49. Introducerea unei imagini faciale identificate în RIF se efectuează cu consemnarea, după caz, a următoarelor elemente:

49.1. numărul de referință;

49.2. sursa și temeiul introducerii;

49.3. autoritatea sau entitatea care a furnizat datele;

49.4. categoria persoanei, potrivit legii speciale privind cooperarea polițienească internațională și actelor normative adoptate în executarea acesteia;

49.5. identificatorii asociați cazului, procedurii sau lucrării, după caz;

49.6. data și ora introducerii;

49.7. registratorul care a efectuat operațiunea;

49.8. alte metadate necesare asigurării trasabilității și utilizării conforme a datelor.

50. Introducerea unei imagini faciale neidentificate în RIF se efectuează cu marcarea distinctă a acesteia ca imagine facială neidentificată, fără asocierea prematură cu identitatea unei persoane, și cu consemnarea contextului de colectare, a sursei, a cauzei sau situației în care a fost obținută, precum și a altor metadate relevante.

51. Imaginile faciale neidentificate se marchează distinct la introducerea în RIF și se recunosc ca atare pe întreaga durată a prelucrării, până la identificarea persoanei sau până la radierea ori arhivarea datelor, în condițiile legii.

52. Numărul de referință se atribuie la momentul introducerii în RIF și se utilizează ca identificator unic al obiectului informațional, inclusiv pentru corelarea acestuia cu datele de bază și informațiile suplimentare care pot fi extrase ulterior, în condițiile legii.

53. Numărul de referință este utilizat ca element de legătură pentru corelarea controlată cu metadatele, rezultatele comparării automatizate, înregistrările privind validarea concordanței și, după caz, datele de bază ori informațiile suplimentare care pot fi extrase ulterior, în condițiile legii.

54. Numărul de referință se atribuie o singură dată, se păstrează pe întreaga durată a evidenței obiectului informațional și nu se reutilizează pentru un alt obiect informațional.

55. Introducerea datelor în setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier se efectuează numai pentru categoriile de persoane prevăzute de lege și numai dacă sunt întrunite condițiile juridice, tehnice și organizatorice aplicabile.

56. Setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier se constituie numai din datele de referință privind imaginile faciale ale persoanelor care au calitatea de bănuit, învinuit sau inculpat, ale persoanelor condamnate pentru săvârșirea infracțiunilor, precum și, după caz, ale victimei, în măsură în care cadrul normativ național permite acest lucru.

57. Datele introduse în setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier nu pot include date de identificare directă a persoanei și se limitează la datele de referință și la elementele tehnice strict necesare efectuării căutării automatizate și administrării fluxului de schimb. Datele de bază și informațiile suplimentare pot fi extrase și furnizate numai ulterior confirmării concordanței și numai în condițiile legii.

Secțiunea a 3-a
Actualizarea, rectificarea, completarea și blocarea datelor

58. Datele din RIF se actualizează fără întârzieri nejustificate atunci când:

58.1. au intervenit modificări privind identitatea sau statutul persoanei;

58.2. au fost recepționate date noi ori rezultate suplimentare din activități procedurale, operative, tehnico-științifice sau de expertiză;

58.3. au fost primite date actualizate de la furnizori ori prin intermediul mecanismelor de interoperabilitate;

58.4. modificarea rezultă dintr-un act procedural, act administrativ sau act jurisdicțional;

58.5. este necesară actualizarea setului de date de referință destinat schimbului automatizat transfrontalier.

59. Completarea datelor se efectuează atunci când evidența existentă nu conține toate elementele necesare individualizării obiectului informațional, ale cazului sau ale contextului de prelucrare, cu condiția existenței unui temei legal și a unei surse autorizate.

60. Rectificarea datelor din RIF se efectuează în cazul constatării caracterului inexact, incomplet, neactual ori neconform al acestora, din oficiu sau la sesizarea subiecților competenți, inclusiv a furnizorilor de date, a destinatarilor datelor ori a persoanei vizate, în condițiile legii.

61. Rectificarea se efectuează astfel încât să fie păstrat istoricul operațiunilor și să poată fi identificată atât forma anterioară a datelor, cât și forma rectificată, utilizatorul care a efectuat operațiunea, data și temeiul acesteia.

62. Blocarea datelor din RIF se dispune în cazul în care:

62.1. exactitatea datelor este contestată și verificarea este în curs;

62.2. există indicii că datele au fost introduse, utilizate sau transmise cu încălcarea legii;

62.3. este necesară conservarea datelor în vederea examinării legalității prelucrării, a efectuării controlului, auditului ori a cercetării unui incident de securitate;

62.4. prelucrarea trebuie restricționată în alte cazuri prevăzute de lege.

63. Pe durata blocării, datele nu pot face obiectul unor noi operațiuni de prelucrare, cu excepția stocării, protejării, verificării legalității, exercitării controlului și a altor operațiuni expres permise de lege.

64. În cazul în care datele blocate fac parte și din setul de date de referință destinat schimbului automatizat transfrontalier, acestea se suspendă sau se retrag din componenta respectivă, în măsura necesară prevenirii unei prelucrări neconforme.

Secțiunea a 4-a
Radierea, arhivarea și păstrarea datelor

65. Radierea datelor din RIF se efectuează în cazul în care:

65.1. a fost constatată lipsa temeiului legal pentru prelucrare;

65.2. datele au fost introduse eronat sau duplicat și nu se justifică păstrarea lor distinctă;

65.3. scopul pentru care au fost prelucrate a fost realizat, iar păstrarea lor ulterioară nu mai are temei legal;

65.4. a expirat termenul de păstrare aplicabil;

65.5. radierea rezultă dintr-un act procedural, act administrativ, hotărâre judecătorească sau din alt temei prevăzut de lege.

66. Radierea datelor din componenta națională a RIF atrage, după caz, radierea sau actualizarea corespunzătoare a datelor din setul de date de referință destinat schimbului automatizat transfrontalier, fără întârzieri nejustificate.

67. Înainte de radierea definitivă, datele pot fi arhivate sau menținute în regim restricționat, în măsura în care acest lucru este necesar pentru respectarea obligațiilor legale privind arhivarea, controlul, auditul, răspunderea juridică sau apărarea drepturilor și intereselor legitime.

68. Arhivarea datelor și documentelor aferente RIF se efectuează în conformitate cu legislația privind arhivarea, nomenclatorul documentelor și regulile interne aprobate de posesor, cu asigurarea confidențialității, integrității și accesului restricționat.

69. Termenele de păstrare a datelor gestionate în RIF se stabilesc diferențiat, în funcție de categoria obiectului informațional, temeiul prelucrării, scopul urmărit, stadiul procedurilor relevante și exigențele cadrului normativ aplicabil.

70. După expirarea termenelor de păstrare aplicabile, datele se radiază, se arhivează sau, după caz, se depersonalizează ireversibil, în condițiile legii, păstrându-se doar evidențele tehnice și metadatele necesare pentru audit, control, constatarea răspunderii ori raportare statistică, în măsura permisă de cadrul normativ aplicabil

71. Datele din RIF se păstrează numai pe perioada necesară realizării scopurilor pentru care au fost colectate și prelucrate, potrivit prezentului Regulament. După expirarea termenelor de păstrare aplicabile, datele se radiază, se arhivează sau, după caz, se depersonalizează ireversibil, păstrându-se exclusiv metadatele statistice necesare pentru audit și raportare, în condițiile legii, ale nomenclatorului arhivistic și ale procedurilor aprobate de posesorul RIF. Prelungirea termenului de păstrare este admisă numai în cazurile justificate prin existența unei cauze penale, a unui dosar de căutare, a unei proceduri judiciare ori a altui temei legal expres.

Secțiunea a 5-a
Evidența operațiunilor asupra datelor

72. SI RIF asigură evidența automată a tuturor operațiunilor efectuate asupra datelor, inclusiv a operațiunilor de introducere, actualizare, rectificare, completare, blocare, radiere, arhivare, consultare, extragere, comparare, validare și transmitere.

73. Evidența operațiunilor asupra datelor trebuie să permită identificarea cel puțin a:

73.1. utilizatorului care a efectuat operațiunea;

73.2. rolului și instituției din care face parte utilizatorul;

73.3. datei și orei operațiunii;

73.4. tipului operațiunii efectuate;

73.5. obiectului informațional vizat;

73.6. temeiului sau justificării operațiunii, după caz;

73.7. sursei datelor ori destinatarului acestora, după caz;

73.8. rezultatului operațiunii.

74. Jurnalele operațiunilor și istoricul modificărilor se păstrează separat și securizat, cu acces limitat la persoanele autorizate în scop de administrare tehnică, control, audit, investigare a incidentelor de securitate ori verificare a legalității prelucrării.

75. Modificarea, ștergerea sau denaturarea neautorizată a evidențelor privind operațiunile asupra datelor este interzisă și atrage răspunderea prevăzută de lege.

76. Regulile tehnice privind formatele de evidență, păstrarea istoriei modificărilor, gestionarea versiunilor, copiile de siguranță și restabilirea datelor se stabilesc de către deținător,

cu aprobarea posesorului, în conformitate cu prezentul Regulament și cu cerințele aplicabile de securitate a informației și protecție a datelor cu caracter personal.

Capitolul V. Accesul la datele din RIF și utilizarea acestora

Secțiunea 1

Dispoziții generale privind accesul la datele din RIF

77. Accesul la datele din RIF se acordă numai persoanelor autorizate, în limitele competențelor prevăzute de lege, ale atribuțiilor funcționale și ale profilului de acces aprobat.

78. Accesul la datele din RIF se realizează diferențiat, în funcție de calitatea subiectului raporturilor juridice în domeniul ținerii registrului, de necesitatea funcțională și de categoria datelor accesate.

79. Accesul la datele din RIF se acordă exclusiv în scopul exercitării atribuțiilor de serviciu și numai pentru realizarea scopurilor prevăzute de lege și de prezentul Regulament.

80. Datele din RIF, inclusiv imaginile faciale, datele de referință privind imaginile faciale, metadatele aferente, informațiile privind rezultatele comparării automatizate și cele privind confirmarea ori infirmarea concordanței, se accesează în condițiile respectării legislației privind protecția datelor cu caracter personal, accesul la informațiile de interes public, securitatea cibernetică și cooperarea polițienească internațională.

81. Accesul la setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier se acordă și se exercită distinct de accesul la componenta națională a registrului, potrivit competențelor stabilite de lege și prezentul Regulament.

82. Datele de referință privind imaginile faciale destinate schimbului automatizat transfrontalier nu pot fi utilizate pentru identificarea directă a persoanei și nu pot fi accesate în afara procedurilor și canalelor stabilite de cadrul normativ aplicabil.

Secțiunea a 2-a

Categoriile de acces și profilurile de acces

83. În funcție de competențele legale și de necesitatea funcțională, accesul la datele din RIF poate include, după caz, următoarele categorii de operațiuni:

83.1. vizualizarea datelor;

83.2. introducerea datelor;

83.3. actualizarea, rectificarea și completarea datelor;

83.4. blocarea datelor;

83.5. radierea datelor, în cazurile prevăzute de lege;

83.6. extragerea datelor și generarea documentelor de ieșire;

83.7. inițierea și gestionarea solicitărilor de comparare automatizată, în limitele competenței;

83.8. validarea concordanței, în cazul personalului calificat desemnat în acest scop;

83.9. administrarea utilizatorilor, rolurilor și profilurilor de acces;

83.10. monitorizarea, controlul și auditul utilizării sistemului.

84. Profilul de acces se stabilește individual pentru fiecare utilizator, în funcție de:

84.1. funcția deținută;

84.2. atribuțiile legale și de serviciu;

84.3. categoria datelor necesare exercitării atribuțiilor;

84.4. nivelul de competență operațională sau tehnică;

84.5. necesitatea de a cunoaște datele respective pentru realizarea unei sarcini concrete.

85. Acordarea, modificarea, suspendarea și revocarea profilurilor de acces se efectuează în condițiile stabilite de posesor, prin act administrativ intern sau prin proceduri aprobate de acesta, cu implicarea deținătorului, după caz.

86. Fiecărui utilizator i se atribuie un identificator unic de acces, individual și netransmisibil. Utilizarea acreditărilor altei persoane, partajarea acestora ori permiterea accesului prin intermediul propriului cont unei alte persoane este interzisă.

87. Accesul utilizatorilor la funcționalitățile SI RIF se realizează prin mijloace de autentificare și control al accesului conforme cadrului normativ aplicabil și politicilor de securitate aprobate.

88. Dreptul de acces la datele din RIF nu are caracter permanent și se menține doar pe perioada existenței temeiului juridic și a necesității funcționale care au justificat acordarea acestuia.

Secțiunea a 3-a
Acordarea și exercitarea accesului la date

89. Accesul la datele din RIF se acordă la solicitarea motivată a conducătorului autorității ori entității interesate sau a persoanei împuternicite de acesta, cu indicarea temeiului legal, a scopului accesului, a categoriilor de date necesare și a persoanelor pentru care se solicită profiluri de acces.

90. Posesorul, cu participarea deținătorului, după caz, examinează solicitarea de acces și decide asupra acordării, limitării sau refuzului accesului, în funcție de:

90.1. existența competenței legale;

90.2. compatibilitatea scopului declarat cu scopurile registrului;

90.3. caracterul necesar și proporțional al accesului solicitat;

90.4. disponibilitatea măsurilor tehnice și organizatorice necesare pentru utilizarea legală și securizată a datelor.

91. Refuzul acordării accesului se dispune în cazul în care nu este demonstrată competența legală, nu este justificată necesitatea funcțională ori nu sunt întrunite condițiile de securitate și conformitate necesare.

92. Accesul acordat poate fi limitat la anumite categorii de date, la anumite funcționalități, la anumite cauze ori situații, la anumite intervale de timp sau la alte restricții necesare pentru respectarea principiului minimizării datelor.

93. Utilizatorii autorizați accesează datele din RIF numai în legătură cu o sarcină concretă de serviciu, cu o procedură legală determinată ori, după caz, cu un caz individual documentat.

94. Accesarea datelor în scop de verificare generală, exploratorie, statistică individualizată neautorizată ori în alte scopuri incompatibile cu temeiul legal al prelucrării este interzisă.

95. În cazul accesului la datele necesare cooperării polițienești internaționale, inclusiv la setul de date de referință destinat schimbului automatizat transfrontalier, utilizatorii acționează numai prin intermediul punctelor de contact, al canalelor securizate și al procedurilor stabilite de lege și de tratatele internaționale aplicabile.

Secțiunea a 4-a
Punerea la dispoziție și furnizarea datelor din RIF

96. Datele din RIF pot fi puse la dispoziția subiecților îndreptățiți prin:

96.1. acces direct și autorizat la interfețele sistemului, conform profilului de acces;

96.2. extrase, rapoarte sau alte documente de ieșire generate de sistem;

96.3. schimb automatizat de date, prin mecanisme de interoperabilitate, în condițiile legii;

96.4. alte modalități prevăzute expres de cadrul normativ aplicabil.

97. Furnizarea datelor din RIF către autorități, instituții sau alte entități se realizează numai în măsura în care acestea sunt îndreptățite prin lege sau prin tratatele internaționale la care Republica Moldova este parte și numai pentru realizarea atribuțiilor lor legale.

98. Datele obținute din RIF se furnizează în volumul minim necesar scopului pentru care sunt solicitate.

99. Datele de identificare directă ale persoanei și alte informații suplimentare asociate unei imagini faciale pot fi furnizate numai în condițiile legii, inclusiv, după caz, ulterior confirmării concordanței și numai subiecților care au competența legală de a primi asemenea date.

100. Datele primite din RIF nu pot fi transmise mai departe către alte autorități, entități sau persoane, decât în cazurile prevăzute expres de lege ori cu autorizarea prealabilă a autorității furnizoare, atunci când cadrul normativ aplicabil impune o asemenea condiție.

101.În cadrul schimbului automatizat transfrontalier, utilizarea și furnizarea ulterioară a datelor se efectuează cu respectarea restricțiilor, condițiilor și limitărilor comunicate de autoritatea furnizoare și a cadrului normativ aplicabil cooperării polițienești internaționale.

Secțiunea a 5-a
Utilizarea datelor din RIF și restricțiile aplicabile

102.Datele din RIF se utilizează exclusiv pentru:

102.1. prevenirea, constatarea și investigarea infracțiunilor;

102.2. identificarea ori verificarea identității persoanelor, în condițiile legii;

102.3. căutarea persoanelor dispărute;

102.4. identificarea cadavrelor ori a părților acestora;

102.5. efectuarea comparării biometrice faciale și validarea concordanței, în condițiile prezentului Regulament;

102.6. realizarea schimbului automatizat al datelor de referință privind imaginile faciale, în condițiile legii;

102.7. alte scopuri expres prevăzute de lege și compatibile cu destinația registrului.

103.Utilizarea datelor din RIF în alte scopuri decât cele prevăzute în prezenta secțiune și de cadrul normativ aplicabil este interzisă.

104.Este interzisă utilizarea datelor din RIF:

104.1. pentru supraveghere generalizată nediferențiată;

104.2. pentru interogări exploratorii sau nedeterminate;

104.3. pentru crearea de profiluri discriminatorii;

104.4. pentru luarea unei decizii care produce efecte juridice sau afectează semnificativ persoana exclusiv în temeiul unui rezultat automatizat nevalidat, în cazurile în care legea impune verificare umană;

104.5. cu încălcarea restricțiilor de acces, a obligațiilor de confidențialitate sau a condițiilor stabilite de autoritatea furnizoare.

105.Utilizatorii și destinatarii datelor din RIF sunt obligați:

105.1. să utilizeze datele numai în scopurile și limitele pentru care le-au fost puse la dispoziție;

105.2. să păstreze confidențialitatea datelor și să prevină divulgarea neautorizată a acestora;

105.3. să aplice măsuri tehnice și organizatorice adecvate pentru protecția datelor;

105.4. să informeze fără întârziere posesorul sau deținătorul despre orice acces neautorizat, incident de securitate, eroare ori neconcordanță constatată;

105.5. să nu modifice, copieze, exporte, distribuie sau stocheze datele în afara condițiilor legale și a profilului de acces acordat.

106.Persoana vizată poate exercita drepturile privind informarea, accesul, rectificarea, completarea, restricționarea prelucrării, opoziția, ștergerea, precum și dreptul de contestare, în condițiile și limitele stabilite de legislația privind protecția datelor cu caracter personal și de normele speciale aplicabile activităților de prevenire, constatare și investigare a infracțiunilor.

Secțiunea a 6-a
Suspendarea și revocarea accesului

107.Accesul la datele din RIF se suspendă sau se revocă, după caz, în următoarele situații:

107.1. încetarea raporturilor de serviciu ori modificarea atribuțiilor persoanei;

107.2. dispariția temeiului legal ori a necesității funcționale care au justificat acordarea accesului;

107.3. constatarea utilizării neconforme sau abuzive a datelor;

107.4. nerespectarea obligațiilor de confidențialitate și securitate;

107.5. apariția unor riscuri de securitate care impun restrângerea imediată a accesului;

107.6. alte cazuri prevăzute de lege sau de actele administrative interne adoptate în temeiul acesteia.

108.Suspendarea sau revocarea accesului nu exonerează persoana de răspunderea pentru operațiunile efectuate anterior și nu aduce atingere obligației de păstrare a confidențialității datelor la care a avut acces.

109.Orice acordare, modificare, suspendare sau revocare a drepturilor de acces se consemnează în evidențele sistemului și în documentele interne aferente administrării utilizatorilor și profilurilor de acces.

Capitolul VI. Compararea automatizată, validarea concordanței și evidența rezultatelor

Secțiunea 1

Dispoziții generale privind compararea automatizată

110.Compararea automatizată a imaginilor faciale în cadrul RIF reprezintă operațiunea tehnică realizată prin intermediul SI RIF, prin care imaginea facială supusă verificării este comparată cu datele comparative disponibile în sistem, în vederea stabilirii existenței unei posibile concordanțe.

111.Compararea automatizată se realizează numai în scopurile prevăzute de lege, în limitele competenței autorității solicitante și cu respectarea principiilor legalității, necesității, proporționalității, limitării scopului, minimizării datelor, trasabilității și securității informației.

112.Compararea automatizată poate fi efectuată:

112.1. în cadrul componentei naționale a RIF;

112.2. în cadrul mecanismului de căutare automatizată a datelor de referință privind imaginile faciale destinat schimbului automatizat transfrontalier, în condițiile legii;

112.3. prin corelarea controlată cu date și metadate relevante din sisteme informaționale și resurse informaționale interoperabile, în măsura permisă de lege.

113.Compararea automatizată se efectuează exclusiv în legătură cu un caz individual determinat și documentat. Inițierea unor interogări generale, exploratorii, preventive nedeterminate sau în alte scopuri incompatibile cu cadrul normativ aplicabil este interzisă.

114.Compararea automatizată a imaginilor faciale nu poate produce, prin ea însăși, efecte operaționale definitive în lipsa validării umane a concordanței, în cazurile în care legea sau prezentul Regulament impun o asemenea verificare.

Secțiunea a 2-a

Inițierea comparării automatizate

115.Compararea automatizată se inițiază de către utilizatorii autorizați, în limitele rolului și profilului de acces atribuit, în baza unui temei legal și a unei necesități funcționale concrete.

116.Solicitarea de comparare automatizată trebuie să permită identificarea cel puțin a:

116.1. autorității sau entității solicitante;

116.2. utilizatorului care inițiază operațiunea;

116.3. cazului individual în legătură cu care se solicită compararea;

116.4. imaginii faciale supuse comparării;

116.5. temeiului legal și scopului operațiunii;

116.6. datei și orei inițierii;

116.7. altor metadate necesare urmăririi fluxului operațional.

117.Înainte de inițierea comparării automatizate, utilizatorul autorizat verifică, după caz:

117.1. calitatea suficientă a imaginii faciale pentru comparare;

117.2. existența temeiului legal și a cazului individual;

117.3. încadrarea solicitării în limitele competenței sale;

117.4. faptul că datele utilizate sunt necesare și relevante pentru scopul urmărit;

117.5. faptul că solicitarea nu constituie o interogare exploratorie ori discriminatorie.

118.Imaginile faciale neidentificate pot face obiectul comparării automatizate cu menținerea marcării lor distincte pe întreaga durată a prelucrării, până la eventuala identificare ulterioară a persoanei, în condițiile legii.

119.În cadrul mecanismului de căutare automatizată transfrontalieră, solicitarea se formulează și se transmite numai prin canalele, punctele de contact și procedurile stabilite de lege și de actele normative subsecvente.

Secțiunea a 3-a
Efectuarea comparării automatizate și
formarea rezultatului

120.Compararea automatizată a imaginilor faciale se efectuează prin intermediul componentei de comparare biometrică facială a SI RIF, inclusiv prin mecanisme tehnice de tip 1:1 și 1:N, în funcție de tipul solicitării și scopul urmărit.

121.În procesul comparării automatizate, SI RIF realizează, după caz:

121.1. contrapunerea imaginii faciale supuse verificării cu mostrele comparative disponibile;

121.2. determinarea nivelului de asemănare;

121.3. formarea rezultatului comparării;

121.4. generarea listei mostrelor comparative pentru care există posibilitatea unei concordanțe;

121.5. înregistrarea rezultatului comparării și a metadatelor aferente.

122.Rezultatul comparării automatizate poate consta, după caz, în:

122.1. inexistența unei concordanțe;

122.2. existența unei concordanțe posibile;

122.3. existența mai multor concordanțe posibile;

122.4. imposibilitatea tehnică de formare a unui rezultat concludent.

123.Rezultatul comparării automatizate se înregistrează în RIF cu indicarea cel puțin a:

123.1. identificatorului rezultatului comparării;

123.2. numărului de referință al imaginii faciale supuse comparării;

123.3. numărului de referință al mostrei comparative sau al mostrelor comparative relevante, după caz;

123.4. datei și orei comparării;

123.5. tipului și statutului rezultatului;

123.6. nivelului de asemănare, după caz;

123.7. componentei tehnice prin care a fost generat rezultatul;

123.8. utilizatorului sau procesului tehnic care a inițiat operațiunea.

124.Rezultatul comparării automatizate are caracter preliminar până la validarea acestuia de către personal calificat, în cazurile în care este necesară confirmarea concordanței.

125.În cazul mecanismului de căutare automatizată transfrontalieră, răspunsul generat în etapa de căutare conține numai datele strict necesare identificării solicitării, urmăririi fluxului de schimb și gestionării concordanței, fără a permite identificarea directă a persoanei, în condițiile legii.

Secțiunea a 4-a
Lista mostrelor pentru care există posibilitatea unei concordanțe

126. Lista mostrelor pentru care există posibilitatea unei concordanțe reprezintă rezultatul tehnic intermediar al comparării automatizate, format din una sau mai multe mostre comparative selectate de SI RIF în baza nivelului de asemănare determinat potrivit regulilor de procesare aplicabile.

127. Lista mostrelor pentru care există posibilitatea unei concordanțe nu constituie, prin ea însăși, concordanță confirmată și nu produce efecte juridice, procesuale, operaționale sau administrative până la validarea concordanței de către personal calificat.

128. Lista mostrelor pentru care există posibilitatea unei concordanțe se formează exclusiv în raport cu un caz individual, în condițiile legii, și include mostrele comparative selectate automat de sistem în ordinea descrescătoare a nivelului de asemănare. Numărul maxim al mostrelor incluse

în listă, precum și pragurile tehnice aplicabile formării acesteia, se stabilesc prin documentația tehnică a SI RIF, aprobată în condițiile legii.

129. Accesul la lista mostrelor pentru care există posibilitatea unei concordanțe este permis numai personalului calificat desemnat pentru validarea concordanței și altor utilizatori autorizați expres, în limitele rolurilor și profilurilor de acces atribuite, cu respectarea cerințelor de jurnalizare și trasabilitate.

130. Până la confirmarea concordanței, în baza listei mostrelor pentru care există posibilitatea unei concordanțe:

130.1. nu se extrag și nu se furnizează datele de identificare directă ale persoanei;

130.2. nu se furnizează informații suplimentare din sistemele-sursă interoperabile, cu excepția celor strict necesare procesului de validare, în condițiile legii;

130.3. nu se dispune și nu se fundamentează exclusiv nicio măsură procesuală, operativă sau administrativă.

131. Validarea concordanței se efectuează prin revizuirea manuală a rezultatului comparării automatizate și, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe, cu consemnarea obligatorie în sistem a:

131.1. identității sau identificatorului utilizatorului care a efectuat validarea;

131.2. datei și orei validării;

131.3. mostrei ori mostrelor examinate;

131.4. rezultatului validării – confirmare, infirmare sau rezultat neconcludent;

131.5. observațiilor relevante care au fundamentat validarea, după caz.

132. În cazul infirmării concordanței, lista mostrelor pentru care există posibilitatea unei concordanțe păstrează statutul de rezultat tehnic intermediar și poate fi utilizată numai în scopuri de jurnalizare, control, audit, verificare ulterioară a legalității prelucrării și îmbunătățire a funcționării sistemului, în condițiile legii.

133. În cazul confirmării concordanței, extragerea și furnizarea datelor de bază și a informațiilor suplimentare se realizează numai în condițiile prezentului Regulament, ale legii speciale privind cooperarea polițienească internațională și ale actelor normative aplicabile.

Secțiunea a 5-a
Validarea concordanței

134. Validarea concordanței reprezintă verificarea umană a rezultatului comparării automatizate și, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe, de către personal calificat, în vederea confirmării, infirmării concordanței ori constatării unui rezultat neconcludent.

135. Validarea concordanței se efectuează numai de către personal calificat, desemnat prin act administrativ al autorității competente, care a urmat instruirea necesară pentru utilizarea SI RIF, interpretarea rezultatelor comparării biometrice faciale, aplicarea cerințelor de protecție a datelor și respectarea procedurilor de jurnalizare și trasabilitate.

136. Validarea concordanței este obligatorie în toate cazurile în care rezultatul comparării automatizate este utilizat pentru:

136.1. identificarea ori verificarea identității unei persoane;

136.2. individualizarea unui caz;

136.3. extragerea datelor de bază sau a informațiilor suplimentare;

136.4. furnizarea unor date în cadrul cooperării polițienești internaționale;

136.5. luarea unei măsuri operaționale ori procedurale care poate produce efecte juridice sau factuale relevante.

137. În procesul validării concordanței, personalul calificat examinează cel puțin:

137.1. imaginea facială supusă comparării;

137.2. mostra sau mostrele comparative indicate de sistem;

137.3. nivelul de asemănare și relevanța rezultatului tehnic;

137.4. calitatea imaginilor comparate;

137.5. contextul cazului individual;

137.6. existența unor elemente care pot conduce la confuzie, eroare sau concluzii neveridice.

138.În urma validării, rezultatul se consemnează ca:

138.1. concordanță confirmată;

138.2. concordanță infirmată;

138.3. rezultat neconcludent, atunci când datele disponibile nu permit o concluzie suficient de certă și sunt necesare verificări suplimentare.

139.În cazul în care autoritatea competentă a Republicii Moldova are calitatea de autoritate solicitată în cadrul schimbului automatizat transfrontalier, confirmarea concordanței se efectuează numai după revizuirea manuală a rezultatului comparării automatizate și, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe, de către cel puțin un membru calificat al personalului, în condițiile legii.

140.Confirmarea concordanței nu echivalează, prin ea însăși, cu stabilirea definitivă a identității persoanei în afara cadrului procedural aplicabil și nu substituie alte verificări, expertize sau acte procedurale cerute de lege.

141.În situația infirmării concordanței, rezultatul comparării nu poate fi utilizat ca temei pentru extragerea ori furnizarea datelor de bază și a informațiilor suplimentare, cu excepția păstrării sale în evidențele sistemului pentru trasabilitate, control și audit.

Secțiunea a 6-a
Evidența rezultatelor comparării și a validării

142.SI RIF asigură evidența distinctă a:

142.1. solicitărilor de comparare automatizată;

142.2. rezultatelor comparării automatizate;

142.3. validărilor efectuate;

142.4. confirmărilor sau infirmărilor concordanței;

142.5. operațiunilor ulterioare efectuate în legătură cu rezultatele comparării și validării.

143.Înregistrarea privind confirmarea sau infirmarea concordanței cuprinde cel puțin:

143.1. identificatorul validării;

143.2. identificatorul rezultatului comparării;

143.3. data și ora validării;

143.4. rezultatul validării;

143.5. datele privind persoana calificată care a efectuat validarea;

143.6. observațiile relevante privind motivarea confirmării sau infirmării, după caz;

143.7. legătura cu cazul individual și cu eventualele operațiuni ulterioare.

144.Toate rezultatele comparării și validării se păstrează în RIF cu asigurarea istoricului operațiunilor, a trasabilității complete și a posibilității verificării ulterioare în scop de control, audit, investigare a incidentelor de securitate ori verificare a legalității prelucrării.

145.Rezultatele comparării automatizate și ale validării concordanței pot fi utilizate pentru extragerea datelor de bază și a informațiilor suplimentare numai în măsura în care concordanța a fost confirmată și numai în condițiile legii și ale prezentului Regulament.

146.În cazul existenței unei concordanțe confirmate în cadrul mecanismului de schimb automatizat transfrontalier, furnizarea ulterioară a datelor de bază și a informațiilor suplimentare se realizează prin canalele, procedurile și punctele de contact stabilite de lege și de actele normative subsecvente.

147.Regulile tehnice privind pragurile operaționale, parametrii de comparare, criteriile minime de calitate a imaginilor, formatele de evidență a rezultatelor, statuturile operaționale și fluxurile interne de validare se stabilesc prin documentația tehnică a SI RIF și prin actele administrative aprobate în temeiul prezentului Regulament, cu respectarea legii.

Capitolul VII. Interoperabilitatea și schimbul de date
Secțiunea 1

Dispoziții generale

148.Interoperabilitatea și schimbul de date în cadrul RIF se realizează în scopul asigurării funcționării SI RIF ca resursă informațională specializată de stat, al formării și actualizării datelor, al identificării ori verificării identității persoanelor, al căutării persoanelor dispărute, al identificării cadavrelor ori a părților acestora, precum și al realizării cooperării polițienești internaționale, în condițiile legii.

149.Interoperabilitatea SI RIF se asigură, după caz:

149.1. la nivel național, prin schimbul de date cu sisteme informaționale și resurse informaționale relevante ale statului;

149.2. la nivel transfrontalier, prin mecanismele de căutare și schimb automatizat al datelor de referință privind imaginile faciale și prin furnizarea ulterioară a datelor de bază și a informațiilor suplimentare, în condițiile cadrului normativ aplicabil cooperării polițienești internaționale.

150.În cadrul schimbului de date se transmit numai datele strict necesare și relevante pentru scopul urmărit, cu respectarea regimului juridic al fiecărei categorii de date și a restricțiilor stabilite de lege ori de autoritatea furnizoare, după caz.

151.Interoperabilitatea și schimbul de date nu pot avea ca efect extinderea competențelor legale ale autorităților ori entităților participante și nu pot substitui temeiul juridic necesar pentru accesarea, utilizarea ori furnizarea datelor.

Secțiunea a 2-a
Interoperabilitatea la nivel național

152.Dacă, pentru introducerea, actualizarea, rectificarea, completarea, blocarea, radierea ori utilizarea datelor în RIF, legislația prevede deținerea unor date sau documente disponibile în resursele informaționale ale altor autorități ori entități publice, acestea se consumă sau se furnizează prin intermediul platformei guvernamentale de interoperabilitate (MConnect), în condițiile legii.

153.Pentru expunerea și consumul evenimentelor de sistem relevante pentru interoperabilitate, SI RIF poate utiliza componenta MConnect Events, prin interfețe de programare a aplicațiilor (API), în condițiile cadrului normativ aplicabil, ale ghidului tehnic publicat de Instituția publică „Agenția de Guvernare Electronică”, ale cerințelor de securitate, ale acordurilor/contractelor de schimb de date și ale documentației tehnice aferente SI RIF.

154.Evenimentele de sistem expuse prin MConnect Events se stabilesc în documentația tehnică aferentă SI RIF și se limitează la evenimentele necesare pentru realizarea interoperabilității, cu respectarea regimului juridic al datelor, a principiului necesității și proporționalității, a cerințelor de protecție a datelor cu caracter personal, securitate cibernetică, jurnalizare și trasabilitate.

155.Interoperabilitatea la nivel național se realizează numai cu sisteme informaționale și resurse informaționale relevante pentru scopurile registrului, fără a substitui funcțiile de evidență primară ale acestora și fără a afecta regimul juridic propriu al datelor gestionate de ele.

156.În cadrul interoperabilității la nivel național, SI RIF poate consuma sau furniza, după caz:

156.1. date de identificare necesare verificării identității persoanei;

156.2. date și documente necesare individualizării cazului;

156.3. date necesare actualizării și rectificării înregistrărilor;

156.4. date necesare verificării calității și coerenței evidențelor;

156.5. alte date prevăzute de lege, în măsura în care sunt necesare realizării atribuțiilor autorităților competente.

157.Schimbul de date prin interoperabilitate la nivel național se efectuează pe baza serviciilor de platformă, interfețelor tehnice, regulilor de validare, nomenclatoarelor și specificațiilor aprobate potrivit cadrului normativ aplicabil.

158.Subiecții care participă la formarea și actualizarea RIF prin consumul ori furnizarea datelor prin interoperabilitate sunt autoritățile și entitățile publice care dețin, administrează ori

gestionează sisteme informaționale și resurse informaționale relevante, în limitele competențelor prevăzute de lege.

159.În cazul în care, prin interoperabilitate, sunt recepționate date care indică neconcordanțe, erori sau necesitatea unor verificări suplimentare, acestea se supun procedurilor interne de verificare, rectificare ori actualizare prevăzute de prezentul Regulament.

Secțiunea a 3-a
Furnizarea și consumul de date la nivel național

160.Furnizarea datelor din RIF către autorități și entități publice la nivel național se realizează numai dacă acestea sunt competente prin lege să primească asemenea date și numai în măsura necesară exercitării atribuțiilor lor.

161.Datele din RIF pot fi puse la dispoziția subiecților autorizați la nivel național prin:

161.1. interoperabilitate, prin intermediul MConnect;

161.2. acces direct și autorizat la interfețele SI RIF, în condițiile profilului de acces acordat;

161.3. extrase, rapoarte sau alte documente generate de sistem, în condițiile legii;

161.4. alte modalități prevăzute expres de cadrul normativ aplicabil.

162.În cadrul furnizării datelor la nivel național, se respectă următoarele reguli:

162.1. se furnizează numai datele strict necesare scopului declarat;

162.2. se aplică, după caz, măsuri de restricționare, pseudonimizare sau limitare a volumului de date;

162.3. se interzice utilizarea datelor în alte scopuri decât cele pentru care au fost solicitate și furnizate;

162.4. fiecare operațiune de furnizare și consum de date este supusă trasabilității și poate fi verificată ulterior.

Secțiunea a 4-a
Schimbul automatizat transfrontalier al datelor de referință privind imaginile faciale

163.SI RIF contribuie, în condițiile legii, tratatelor internaționale și actelor de punere în aplicare, la realizarea schimbului automatizat transfrontalier al datelor de referință privind imaginile faciale, precum și la interacțiunea cu infrastructurile și mecanismele externe utilizate în cooperarea polițienească internațională.

164.Funcționalitățile aferente schimbului automatizat transfrontalier al datelor de referință privind imaginile faciale se pun în aplicare numai după asigurarea condițiilor juridice, organizatorice și tehnice necesare, inclusiv, după caz, a notificărilor, desemnărilor și actelor de punere în aplicare prevăzute de lege.

165.Schimbul automatizat transfrontalier se realizează exclusiv în cazuri individuale, prin intermediul autorității naționale competente și/sau al punctelor de contact competente, precum și prin canalele, infrastructurile și mecanismele stabilite de legea specială privind cooperarea polițienească internațională, de tratatele internaționale și de actele normative subsecvente.

166.În etapa de căutare automatizată transfrontalieră, se transmit și se primesc numai datele de referință privind imaginile faciale și alte date strict necesare identificării solicitării, urmăririi fluxului de schimb și gestionării concordanței, fără a permite identificarea directă a persoanei.

167.Categoriile de persoane ale căror date de referință privind imaginile faciale pot fi incluse în mecanismul de schimb automatizat transfrontalier, precum și condițiile de constituire, păstrare, utilizare, suspendare ori retragere a acestora, se stabilesc prin lege.

168.Transmiterea și primirea datelor de referință privind imaginile faciale în cadrul schimbului automatizat transfrontalier se realizează cu asigurarea confidențialității, integrității și autenticității acestora, inclusiv prin utilizarea criptării și a altor măsuri tehnice și organizatorice adecvate, potrivit legii.

169.SI RIF asigură separarea funcțională și logică dintre componenta națională a registrului și setul de date de referință destinat schimbului automatizat transfrontalier, precum și aplicarea profilurilor de acces și a fluxurilor distincte de utilizare pentru fiecare dintre aceste componente.

Secțiunea a 5-a
Furnizarea datelor de bază și a informațiilor suplimentare ulterior concordanței confirmate

170.Ulterior confirmării concordanței, SI RIF poate fi utilizat pentru extragerea și furnizarea, în condițiile legii, a datelor de bază și a informațiilor suplimentare aferente numărului de referință identificat.

171.Furnizarea datelor de bază și a informațiilor suplimentare ulterior unei concordanțe confirmate se realizează numai:

171.1. subiecților autorizați prin lege;

171.2. prin canalele și procedurile prevăzute pentru cooperarea polițienească internațională;

171.3. în măsura în care datele solicitate sunt necesare și proporționale scopului urmărit;

171.4. cu respectarea restricțiilor și condițiilor stabilite de lege ori, după caz, de autoritatea furnizoare.

172.Confirmarea unei concordanțe nu atrage automat furnizarea tuturor datelor asociate. Furnizarea ulterioară se limitează la datele de bază și informațiile suplimentare strict necesare, în funcție de obiectul solicitării, temeiul legal și competența autorității solicitante.

173.În cazul în care Republica Moldova are calitatea de stat solicitat, furnizarea datelor de bază și a informațiilor suplimentare se efectuează numai după validarea concordanței, prin intermediul punctului de contact competent și în condițiile legii speciale aplicabile cooperării polițienești internaționale.

174.În cazul în care Republica Moldova are calitatea de stat solicitant, datele de bază și informațiile suplimentare primite în urma unei concordanțe confirmate pot fi utilizate numai în scopul pentru care au fost solicitate și numai în limitele stabilite de cadrul normativ aplicabil și de eventualele condiții comunicate de autoritatea furnizoare.

Secțiunea a 6-a
Restricții și evidența schimbului de date

175.Este interzisă utilizarea mecanismelor de interoperabilitate și schimb de date:

175.1. în lipsa unui temei legal;

175.2. în afara competențelor atribuite;

175.3. în scopuri generale, exploratorii ori discriminatorii;

175.4. pentru ocolirea regimului juridic al accesului la date;

175.5. pentru transmiterea unor date excesive ori nerelevante.

176.Orice operațiune de consum, furnizare, transmitere sau recepționare a datelor prin interoperabilitate ori în cadrul schimbului automatizat transfrontalier se înregistrează în evidențele SI RIF, astfel încât să permită identificarea utilizatorului sau a procesului tehnic, a datei și orei operațiunii, a temeiului operațiunii, a categoriei de date schimbate și a destinatarului ori sursei acestora, după caz.

177.Evidențele privind schimbul de date se păstrează în condiții de securitate și pot fi utilizate în scop de control, audit, verificare a legalității prelucrării, investigare a incidentelor de securitate și stabilire a răspunderii, potrivit legii.

178.Cerințele tehnice privind interfețele de interoperabilitate, formatele de schimb, regulile de validare, parametrii operaționali, registrele tehnice ale schimburilor, fluxurile de notificare și alte condiții de implementare se stabilesc prin documentația tehnică a SI RIF și prin actele administrative aprobate în temeiul prezentului Regulament, cu respectarea legii.

Capitolul VIII. Securitatea, jurnalizarea, monitorizarea, controlul și auditul

Secțiunea 1

Dispoziții generale

179.Securitatea, jurnalizarea, monitorizarea, controlul și auditul în cadrul RIF se asigură în scopul garantării legalității prelucrării datelor, al protejării confidențialității, integrității, disponibilității, autenticității și rezilienței SI RIF, al prevenirii accesului neautorizat, al detectării utilizărilor neconforme și al asigurării trasabilității complete a operațiunilor efectuate în sistem.

180.Măsurile de securitate, jurnalizare, monitorizare, control și audit prevăzute în prezentul capitol se aplică întregului ciclu de viață al datelor gestionate prin SI RIF, inclusiv la colectarea, recepționarea, introducerea, stocarea, actualizarea, rectificarea, blocarea, radierea, arhivarea, compararea automatizată, validarea concordanței, interoperabilitatea și schimbul de date.

181.Posesorul, deținătorul, administratorul tehnic, registratorii, furnizorii de date, destinatarii datelor și ceilalți utilizatori autorizați ai SI RIF au obligația să respecte cerințele de securitate, jurnalizare, monitorizare și audit stabilite de prezentul Regulament, de actele administrative aprobate în temeiul acestuia și de legislația aplicabilă în domeniul protecției datelor cu caracter personal și al securității cibernetice.

182.Posesorul aprobă procedurile interne privind securitatea, administrarea accesului, jurnalizarea, monitorizarea și auditul SI RIF, deținătorul asigură implementarea tehnică aplicativă a acestora, iar administratorul tehnic asigură măsurile tehnice aferente infrastructurii administrate, în limitele competențelor stabilite de lege.

183.Înainte de punerea în exploatare a SI RIF și, după caz, înainte de operaționalizarea componentei de schimb automatizat transfrontalier, posesorul asigură evaluarea impactului asupra protecției datelor cu caracter personal, în condițiile Legii nr. 195/2024 privind protecția datelor cu caracter personal, precum și implementarea măsurilor de diminuare a riscurilor identificate.

Secțiunea a 2-a
Măsurile de securitate ale SI RIF

184.SI RIF se exploatează cu aplicarea unor măsuri tehnice și organizatorice adecvate pentru:

183.1. autentificarea utilizatorilor;

183.2. autorizarea și controlul accesului;

183.3. asigurarea confidențialității datelor;

183.4. asigurarea integrității și exactității datelor;

183.5. asigurarea disponibilității și continuității funcționării;

183.6. asigurarea autenticității și trasabilității operațiunilor;

183.7. prevenirea, detectarea și limitarea incidentelor de securitate;

183.8. restabilirea funcționării și recuperarea datelor în caz de incident, avarie sau dezastru.

185.Accesul la funcționalitățile SI RIF se realizează numai prin mecanisme de autentificare și control al accesului conforme cadrului normativ aplicabil și politicilor de securitate aprobate, inclusiv, după caz, prin utilizarea serviciilor guvernamentale comune destinate autentificării.

186.Datele gestionate prin SI RIF se protejează împotriva accesului, copierii, modificării, distrugerii, divulgării, transmiterii sau utilizării neautorizate, inclusiv prin măsuri de segmentare logică, separare a rolurilor, restricționare a privilegiilor, criptare, protecție a comunicațiilor și alte măsuri tehnice adecvate.

187.Componenta națională a RIF și setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier se protejează distinct, prin măsuri diferențiate de acces, utilizare, transmitere și administrare, corespunzător regimului juridic aplicabil fiecărei componente.

188.Găzduirea și exploatarea tehnologică a SI RIF se realizează prin utilizarea platformei tehnologice guvernamentale comune sau a altor infrastructuri permise de cadrul normativ aplicabil, cu respectarea cerințelor de securitate, continuitate operațională și reziliență.

189.Deținătorul asigură efectuarea copiilor de rezervă, menținerea mecanismelor de recuperare a datelor și aplicarea măsurilor de continuitate a funcționării și de restabilire a serviciilor în caz de incidente sau dezastre.

190.În cazul apariției unei amenințări cibernetice, a unui incident de securitate, a unei neconformități grave ori a unui risc iminent pentru legalitatea sau siguranța funcționării SI RIF, deținătorul poate restricționa sau suspenda temporar accesul tehnic la sistem ori la anumite funcționalități ale acestuia, cu informarea imediată a posesorului și cu aplicarea măsurilor de remediere necesare.

Secțiunea a 3-a
Jurnalizarea operațiunilor

191.SI RIF asigură jurnalizarea automată a tuturor operațiunilor relevante efectuate în sistem, inclusiv a celor de autentificare, accesare, consultare, introducere, actualizare, rectificare, blocare, radiere, arhivare, comparare automatizată, validare a concordanței, extragere, furnizare, transmitere, recepționare, suspendare a accesului și administrare a conturilor ori profilurilor de acces.

192.Jurnalizarea trebuie să permită identificarea cel puțin a:

191.1. utilizatorului sau procesului tehnic care a efectuat operațiunea;

191.2. rolului și instituției de apartenență, după caz;

191.3. datei și orei operațiunii;

191.4. tipului operațiunii efectuate;

191.5. obiectului informațional vizat;

191.6. temeiului sau justificării operațiunii, în măsura în care aceasta este asociată unui caz individual ori unei sarcini concrete;

191.7. sursei sau destinatarului datelor, după caz;

191.8. rezultatului operațiunii.

193.Evidențele de jurnalizare se păstrează în condiții de securitate, separat de mediile operaționale, cu protecție împotriva modificării, ștergerii, divulgării ori accesării neautorizate.

194.Jurnalele SI RIF pot fi ținute prin mecanisme interne ale sistemului și, după caz, prin utilizarea serviciilor guvernamentale comune de jurnalizare, în condițiile cadrului normativ aplicabil.

195.Accesul la jurnalele SI RIF este permis numai persoanelor expres autorizate în scop de administrare tehnică, securitate, control intern, audit, investigare a incidentelor, verificare a legalității prelucrării sau stabilire a răspunderii, în condițiile legii.

196.Modificarea, alterarea, ștergerea ori ascunderea neautorizată a înregistrărilor din jurnalele SI RIF este interzisă și atrage răspunderea prevăzută de lege.

Secțiunea a 4-a
Monitorizarea utilizării SI RIF

197.Monitorizarea SI RIF reprezintă activitatea continuă de supraveghere a funcționării tehnice, a utilizării operaționale și a respectării cerințelor de securitate și legalitate în procesul de prelucrare a datelor gestionate prin sistem.

198.Monitorizarea SI RIF are ca obiective:

197.1. verificarea funcționalității continue a sistemului;

197.2. identificarea accesărilor neautorizate sau neobișnuite;

197.3. detectarea incidentelor de securitate, a vulnerabilităților și a neconformităților;

197.4. verificarea respectării profilurilor de acces și a regulilor de utilizare;

197.5. examinarea frecventă a log-urilor și a activităților de prelucrare;

197.6. evaluarea necesității măsurilor de remediere, restricționare ori suspendare a accesului.

199.Posesorul monitorizează implementarea și funcționarea RIF, inclusiv pe componenta de schimb automatizat transfrontalier, iar deținătorul asigură monitorizarea tehnică permanentă a funcționalității sistemului și informează posesorul despre incidentele, deficiențele și riscurile identificate.

200.În cazul constatării unor utilizări neconforme, a unor accesări neautorizate, a unor incidente de securitate sau a altor neconformități, se dispun fără întârziere măsurile necesare pentru limitarea efectelor, remedierea cauzelor, conservarea probelor și, după caz, sesizarea autorităților competente.

Secțiunea a 5-a
Controlul intern și auditul

201.Controlul intern asupra utilizării SI RIF se exercită de către posesor și, după caz, de către alte structuri competente, în limitele atribuțiilor stabilite de lege și de actele administrative interne.

202.Controlul intern vizează, după caz:

201.1. legalitatea accesului și utilizării datelor;

201.2. respectarea profilurilor de acces și a separării rolurilor;

201.3. respectarea procedurilor privind introducerea, actualizarea, rectificarea, blocarea, radierea, compararea, validarea și schimbul de date;

201.4. respectarea cerințelor de securitate și confidențialitate;

201.5. respectarea obligațiilor de jurnalizare și păstrare a evidențelor;

201.6. conformitatea cu prezentul Regulament și cu actele administrative interne adoptate în executarea acestuia.

203.Auditul SI RIF se efectuează periodic sau ori de câte ori este necesar, în scopul evaluării conformității juridice, organizatorice și tehnice a funcționării sistemului, al verificării eficacității măsurilor de securitate și al identificării riscurilor și vulnerabilităților.

204.Auditul poate avea, după caz, caracter tehnic, de securitate, de conformitate, de protecție a datelor cu caracter personal ori mixt, în funcție de obiectul și necesitatea verificării.

205.În cadrul auditului, auditorii sau persoanele împuternicite pot avea acces, în limitele competențelor legale, la configurațiile tehnice, jurnalele sistemului, evidențele operațiunilor, documentele justificative, procedurile interne, registrele de acces, rapoartele de incident și alte materiale necesare verificării.

206.Rezultatele controlului și ale auditului se consemnează în acte de constatare, rapoarte ori alte documente interne, care includ, după caz, neconformitățile identificate, riscurile constatate, măsurile de remediere recomandate, termenele de executare și subiecții responsabili.

207.Posesorul dispune măsurile de remediere necesare în urma constatărilor controlului sau auditului și monitorizează executarea acestora.

Secțiunea a 6-a
Gestionarea incidentelor și răspunderea

208.Orice utilizator, registrator, furnizor de date, destinatar al datelor, administrator tehnic ori alt subiect care constată un incident de securitate, o accesare neautorizată, o pierdere de date, o neconcordanță relevantă ori o utilizare neconformă a SI RIF este obligat să informeze fără întârziere deținătorul și posesorul, potrivit procedurilor interne aplicabile.

209.Gestionarea incidentelor de securitate include, după caz:

208.1. înregistrarea incidentului;

208.2. evaluarea naturii și gravității acestuia;

208.3. limitarea efectelor și izolarea componentelor afectate;

208.4. conservarea urmelor și a dovezilor digitale relevante;

208.5. remedierea cauzelor;

208.6. restabilirea funcționării;

208.7. informarea subiecților competenți și notificarea autorităților competente, în cazurile și condițiile prevăzute de lege.

210.În cazul incidentelor care afectează date cu caracter personal ori securitatea cibernetică, se aplică procedurile de notificare, cooperare și răspuns prevăzute de legislația specială aplicabilă.

211.Utilizarea abuzivă a datelor, accesarea neautorizată a SI RIF, încălcarea obligațiilor de confidențialitate, alterarea jurnalelor, nerespectarea măsurilor de securitate, precum și orice altă prelucrare neconformă a datelor gestionate prin SI RIF atrag răspunderea disciplinară, contravențională, civilă sau penală, după caz, potrivit legii.

212.Cerințele tehnice detaliate privind securitatea, jurnalizarea, monitorizarea, controlul, auditul, copiile de rezervă, continuitatea activității, recuperarea în caz de dezastru și gestionarea incidentelor se stabilesc prin documentația tehnică a SI RIF și prin actele administrative aprobate în temeiul prezentului Regulament.

NOTA DE FUNDAMENTARE
la proiectul hotărârii Guvernului cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ

Proiectul hotărârii Guvernului cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale este elaborat de către Ministerul Afacerilor Interne.

2. Condițiile ce au impus elaborarea proiectului actului normativ

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

Proiectul hotărârii Guvernului cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale a fost elaborat în contextul realizării măsurilor prioritare aferente procesului de aderare a Republicii Moldova la Uniunea Europeană, al alinierii cadrului normativ național la acquis-ul Uniunii Europene în domeniul cooperării polițienești și al schimbului automatizat de date, precum și al implementării angajamentelor asumate în baza Acordului de Asociere între Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, pe de o parte, și Republica Moldova, pe de altă parte.

Sursa proiectului actului normativ derivă din necesitatea realizării angajamentelor asumate de Republica Moldova în procesul de aderare la Uniunea Europeană, în special a celor prevăzute de Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029, aprobat prin Hotărârea Guvernului nr. 306/2025, Cluster 1 Valori fundamentale, Capitolul 24 Justiție, Libertate și Securitate, acțiunea nr. 57, care prevede crearea cadrului necesar pentru gestionarea imaginilor faciale ale persoanelor care au calitatea de bănuit, învinuit sau inculpat, ale persoanelor condamnate și, în măsura permisă de lege, ale victimelor, ca premisă pentru schimbul automatizat al datelor de referință privind imaginile faciale în cadrul mecanismului Prüm II, în conformitate cu Regulamentul (UE) 2024/982.

Proiectul este corelat cu 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, care instituie cadrul normativ european aplicabil schimbului automatizat de profiluri ADN, date dactiloscopice, date privind înmatricularea vehiculelor, imagini faciale și evidențe polițienești.

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

În prezent, cadrul normativ relevant în materia evidenței și prelucrării informațiilor criminalistice și criminologice este instituit prin Legea nr. 216/2003 cu privire la Sistemul informațional integrat automatizat de evidență a infracțiunilor, a cauzelor penale și a persoanelor care au săvârșit infracțiuni, Hotărârea Guvernului nr. 1202/2006 cu privire la aprobarea Concepției Sistemului informațional integrat al organelor de drept, Hotărârea Guvernului nr. 633/2007 cu privire la aprobarea Concepției Sistemului informațional automatizat „Registrul informației criminalistice și criminologice” și Hotărârea Guvernului nr. 328/2012 cu privire la aprobarea Regulamentului privind organizarea și funcționarea Sistemului informațional automatizat „Registrul informației criminalistice și criminologice”. Acest cadru normativ este completat de Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate, precum și Legea nr. 195/2024 privind protecția datelor cu caracter personal.

Cu toate acestea, cadrul normativ existent nu reglementează în mod distinct o *resursă informațională de stat cu destinație departamentală, specializată pentru gestionarea imaginilor faciale ale persoanelor care au calitatea de bănuit, învinuit sau inculpat, ale persoanelor condamnate și, în măsura permisă de lege, ale victimelor, ca premisă pentru*

schimbul automatizat transfrontalier al datelor de referință privind imaginile faciale. În lipsa unui asemenea sistem informațional, imaginile faciale și datele aferente acestora nu sunt reglementate într-o arhitectură unitară, cu reguli clare privind obiectele informaționale, identificatorii, categoriile de date, subiecții implicați, condițiile de acces, procedurile de validare, jurnalizarea operațiunilor, auditul și mecanismele de securitate.

Situația actuală evidențiază existența unor sisteme și resurse informaționale sectoriale relevante pentru activitatea autorităților competente, inclusiv în domeniul evidenței informației criminalistice și criminologice, evidenței dactiloscopice, evidenței genetice judiciare, evidenței populației, migrației și controlului la frontieră. Totuși, aceste sisteme nu au ca obiect principal constituirea și administrarea unei evidențe specializate a imaginilor faciale, a datelor de referință privind imaginile faciale și a mecanismelor de comparare și validare a concordanțelor.

O problemă distinctă constă în *lipsa unei delimitări normative clare între componenta națională de gestionare a imaginilor faciale și setul de date de referință destinat schimbului automatizat transfrontalier*. Componenta națională poate include imagini faciale, metadate și informații asociate necesare realizării atribuțiilor autorităților competente în condițiile legii, inclusiv pentru căutarea persoanelor dispărute și identificarea cadavrelor ori a părților acestora. În schimb, setul de date destinat schimbului automatizat transfrontalier trebuie să fie constituit ca o submulțime distinctă, limitată la categoriile de persoane prevăzute expres de actele normative privind cooperarea polițienească internațională și utilizată exclusiv în condițiile cadrului normativ aplicabil cooperării polițienești internaționale.

De asemenea, cadrul normativ național nu conține un mecanism special pentru atribuirea și utilizarea numerelor de referință aferente imaginilor faciale. În contextul căutării și schimbului automatizat de date, *numărul de referință are un rol esențial*, deoarece permite corelarea controlată a imaginii faciale cu datele de bază și informațiile suplimentare care pot fi extrase ulterior, după confirmarea concordanței și numai în condițiile legii. Numărul de referință *nu trebuie să conțină numele, prenumele, IDNP-ul sau alte date care permit identificarea directă a persoanei,* conform cerințelor cadrului normativ european.

O altă lacună vizează statutul juridic al rezultatului comparării automatizate a imaginilor faciale și al listei mostrelor pentru care există posibilitatea unei concordanțe. În lipsa unei reglementări exprese, există riscul confundării rezultatului tehnic preliminar al comparării automatizate cu o concordanță confirmată. Proiectul soluționează această problemă prin consacrarea expresă a caracterului intermediar al rezultatului tehnic și prin instituirea obligației de validare a concordanței de către personal calificat.

În aceste condiții, intervenția normativă este necesară pentru instituirea unui cadru normativ secundar coerent, *care să permită crearea și funcționarea Sistemului informațional „Registrul imaginilor faciale" (în continuare – SI RIF)* ca resursă informațională specializată de stat cu destinație departamentală, să asigure prelucrarea imaginilor faciale în condiții de legalitate, proporționalitate, securitate și trasabilitate și să creeze premisele juridice, organizaționale și tehnice pentru utilizarea ulterioară a datelor de referință privind imaginile faciale în cadrul cooperării polițienești internaționale.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul hotărârii Guvernului prevede instituirea Sistemului informațional „Registrul imaginilor faciale" și aprobarea a două anexe: Conceptul Sistemului informațional „Registrul imaginilor faciale", conform anexei nr. 1, și Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale, conform anexei nr. 2.

Prin proiect, Ministerul Afacerilor Interne este desemnat în calitate de posesor al SI RIF, cu responsabilitatea de a asigura condițiile juridice, financiare și organizatorice necesare pentru crearea, administrarea, mentenanța și dezvoltarea sistemului. Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne are calitatea de deținător al SI RIF și asigură crearea, dezvoltarea, mentenanța aplicativă, funcționarea tehnică a aplicației, administrarea componentelor software, a bazelor de date, a interfețelor și a mecanismelor aplicative de securitate, jurnalizare, monitorizare și audit. Instituția publică „Serviciul Tehnologia

Informației și Securitate Cibernetică" are calitatea de administrator tehnic și asigură, în limitele competențelor stabilite de cadrul normativ aplicabil, administrarea tehnică a infrastructurii tehnologiilor informaționale aferente găzduirii SI RIF, fără a interveni în administrarea funcțională a datelor gestionate prin RIF.

Totodată, proiectul stabilește că prevederile referitoare la constituirea, utilizarea și schimbul automatizat transfrontalier al setului de date de referință privind imaginile faciale se vor aplica de la data intrării în vigoare a legii privind cooperarea polițienească internațională (înregistrat cu număr unic 264/MAI/2026) și după asigurarea condițiilor juridice, organizatorice și tehnice necesare, precum și aprobarea reglementărilor conform cu standardele Regulamentului (UE) 2024/982 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).

Conceptul SI RIF stabilește cadrul general de creare, dezvoltare și funcționare a sistemului. Acesta reglementează scopul, obiectivele și principiile de funcționare, spațiul juridico-normativ, spațiul funcțional, structura organizațională, documentele și datele utilizate în sistem, spațiul informațional, mecanismele de interoperabilitate, structura informațională și tehnologică, precum și cerințele generale privind securitatea, jurnalizarea, auditul și protecția datelor.

Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale (în continuare – RIF) modul de organizare, ținere, administrare, actualizare, utilizare, furnizare, protecție și arhivare a datelor din RIF. Regulamentul detaliază subiecții raporturilor juridice aferente RIF, drepturile și obligațiile acestora, operațiunile asupra datelor, condițiile de acces, procedura de comparare automatizată, validarea concordanței, regimul listei mostrelor pentru care există posibilitatea unei concordanțe, schimbul de date, interoperabilitatea, securitatea, jurnalizarea, controlul și auditul.

Elementul principal de noutate constă în instituirea unei resurse informaționale de stat cu destinație departamentală, distincte de celelalte sisteme informaționale existente*, destinate evidenței, administrării, comparării, validării și utilizării imaginilor faciale*. SI RIF este conceput ca sistem informațional distinct, specializat și interoperabil cu sistemele informaționale și resursele informaționale relevante ale statului, *fără a substitui funcțiile de evidență primară ale acestora*.

Un alt element nou îl constituie *delimitarea expresă dintre componenta națională a Registrului imaginilor faciale și setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier*. Componenta națională va cuprinde totalitatea imaginilor faciale, metadatelor, informațiilor asociate și rezultatelor comparării automatizate necesare realizării atribuțiilor autorităților competente în condițiile legii. Setul de date de referință destinat schimbului transfrontalier va reprezenta o submulțime distinctă, constituită, păstrată, furnizată și utilizată exclusiv în condițiile actelor normative privind cooperarea polițienească internațională și ale tratatelor internaționale aplicabile.

Proiectul introduce reglementări privind *imaginile faciale identificate și imaginile faciale neidentificate*, inclusiv obligația marcării distincte a imaginilor neidentificate. De asemenea, pentru fiecare imagine facială introdusă în RIF se prevede atribuirea unui număr de referință, utilizat ca identificator al obiectului informațional și ca element de legătură pentru extragerea controlată, după caz, a datelor de bază și a informațiilor suplimentare în cazul unei concordanțe confirmate.

Un element important de noutate îl reprezintă reglementarea expresă a faptului că *datele de referință privind imaginile faciale nu conțin date suplimentare care permit identificarea directă a persoanei*. Datele de identificare și informațiile suplimentare pot fi extrase și furnizate numai ulterior confirmării concordanței și numai în condițiile legii.

Proiectul *reglementează distinct rezultatul tehnic preliminar al comparării automatizate și lista mostrelor pentru care există posibilitatea unei concordanțe*. Lista respectivă este calificată drept rezultat tehnic intermediar, care nu constituie concordanță confirmată și nu produce efecte juridice, procesuale, operaționale sau administrative *până la validarea*

concordanței de către personal calificat. Această soluție introduce o garanție importantă împotriva utilizării automate și nevalidate a rezultatelor generate de sistem.

Prin proiect se *consacră principiul validării umane a concordanței*. Validarea urmează a fi realizată de personal calificat, desemnat și instruit, care aplică procedurile stabilite privind utilizarea SI RIF, interpretarea rezultatului comparării biometrice faciale, protecția datelor, jurnalizarea și trasabilitatea. Numai după confirmarea concordanței poate fi realizată extragerea și furnizarea datelor de bază și a informațiilor suplimentare, în condițiile legii.

Proiectul *reglementează utilizarea obiectelor informaționale împrumutate din alte sisteme informaționale și resurse informaționale de stat*, fără înregistrarea repetată a acestora în RIF. SI RIF păstrează, după caz, numai identificatorii obiectelor împrumutate, datele minime necesare corelării, metadatele privind sursa datelor și informațiile necesare trasabilității accesării ori utilizării acestora. Această soluție este corelată cu principiile evidenței unice, interoperabilității și evitării dublării obiectelor informaționale deja înregistrate în sistemele-sursă.

Proiectul introduce reguli privind *interoperabilitatea SI RIF cu sistemele informaționale și resursele informaționale relevante ale statului*, prin intermediul platformei guvernamentale de interoperabilitate MConnect, inclusiv, după caz, prin componenta MConnect Events, pentru expunerea și consumul evenimentelor de sistem relevante. Totodată, SI RIF utilizează, după caz, serviciile electronice guvernamentale partajate MPass, MSign, MLog, MNotify, MPower și platforma MCloud, cu respectarea cadrului normativ aplicabil, a cerințelor tehnice, de securitate și de trasabilitate.

La proiectarea și dezvoltarea interfețelor SI RIF destinate interacțiunii cu servicii publice electronice ori cu utilizatori externi autorizați se va ține cont, în măsura compatibilă cu destinația și regimul juridic al sistemului, de cerințele privind modelul unitar de design prevăzute de Hotărârea Guvernului nr. 677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design.

În partea ce ține de securitate și protecția datelor, *proiectul instituie reguli privind accesul autorizat și diferențiat, jurnalizarea operațiunilor, trasabilitatea accesărilor, auditul, monitorizarea utilizării sistemului, administrarea rolurilor și profilurilor de acces, precum și aplicarea măsurilor tehnice și organizatorice necesare pentru asigurarea confidențialității, integrității, disponibilității și rezilienței sistemului*. Înainte de punerea în exploatare a SI RIF și, după caz, înainte de operaționalizarea componentei de schimb automatizat transfrontalier, urmează a fi asigurată evaluarea impactului asupra protecției datelor cu caracter personal, potrivit Legii nr. 195/2024 privind protecția datelor cu caracter personal.

Prin urmare, proiectul introduce un cadru normativ complex și specializat pentru funcționarea Registrului imaginilor faciale, cu accent pe legalitatea prelucrării datelor, delimitarea scopurilor, controlul accesului, validarea umană, securitatea informațională, protecția datelor cu caracter personal, interoperabilitatea și crearea premiselor pentru schimbul automatizat transfrontalier al datelor de referință privind imaginile faciale.

Prin proiect se propune ca prezenta hotărâre să intre în vigoare la expirarea termenului de 6 luni de la data publicării în Monitorul Oficial al Republicii Moldova, pentru a fi în concordanță actele normative conexe elaborate în prezent de Ministerul Afacerilor Interne, precum și a condițiilor de elaborare a documentației tehnice. Totodată, proiectul instituie o excepție expresă pentru prevederile referitoare la constituirea, utilizarea și schimbul automatizat transfrontalier al setului de date de referință privind imaginile faciale. Aceste prevederi nu vor deveni aplicabile odată cu intrarea în vigoare generală a hotărârii, ci numai în condițiile stabilite la pct. 4 din proiect, respectiv de la data intrării în vigoare a actului normativ privind cooperarea polițienească internațională și după asigurarea condițiilor juridice, organizatorice și tehnice necesare, inclusiv notificările, actele de punere în aplicare și operaționalizarea mecanismelor externe aplicabile.

Această excepție este justificată prin caracterul complex și condiționat al schimbului automatizat transfrontalier de date privind imaginile faciale. Componenta transfrontalieră

presupune existența unui cadru normativ privind cooperarea polițienească internațională, desemnarea autorităților/punctelor de contact competente, realizarea notificărilor necesare, aprobarea sau aplicarea actelor de punere în aplicare relevante, precum și operaționalizarea mecanismelor tehnice externe aplicabile. În lipsa acestor condiții, aplicarea imediată a prevederilor privind schimbul transfrontalier se consideră prematură și ar putea genera incertitudine în operaționalizare.

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

În procesul de elaborare a proiectului au fost analizate mai multe opțiuni de reglementare, inclusiv opțiunea neintervenției, opțiunea integrării evidenței imaginilor faciale într-un sistem informațional existent, opțiunea reglementării prin acte administrative interne și documentație tehnică, opțiunea reglementării integrale a mecanismelor transfrontaliere prin prezenta hotărâre, precum și opțiunea instituirii unui sistem informațional distinct.

Prima opțiune analizată a fost menținerea situației actuale, fără aprobarea unui act normativ nou. Această opțiune nu a fost reținută, deoarece cadrul normativ existent nu reglementează în mod distinct o resursă informațională specializată pentru evidența, administrarea, compararea biometrică facială, validarea concordanțelor și utilizarea imaginilor faciale. Lipsa intervenției ar menține lacunele privind categoriile de date, obiectele informaționale, subiecții implicați, condițiile de acces, jurnalizarea, auditul, validarea umană și delimitarea dintre componenta națională și setul de date destinat schimbului automatizat transfrontalier.

A doua opțiune analizată a constat în integrarea evidenței imaginilor faciale într-un sistem informațional existent, în special într-un sistem destinat evidenței informației criminalistice, criminologice sau al altor date relevante pentru activitatea organelor de drept. Această opțiune nu a fost reținută, deoarece imaginile faciale și datele de referință aferente acestora necesită o arhitectură funcțională, informațională și juridică distinctă, având în vedere specificul datelor biometrice, necesitatea comparării automatizate, validarea umană a concordanței, atribuirea numerelor de referință și separarea strictă a setului de date destinat schimbului transfrontalier. Integrarea într-un sistem existent ar putea genera suprapuneri de competențe, confuzii privind obiectele informaționale și dificultăți de delimitare între evidențele primare și funcțiile specializate ale registrului imaginilor faciale.

A treia opțiune analizată a fost reglementarea aspectelor aferente imaginilor faciale exclusiv prin acte administrative interne sau prin documentație tehnică. Această opțiune nu a fost reținută, deoarece prelucrarea imaginilor faciale implică date biometrice și poate avea impact asupra drepturilor și libertăților persoanelor. Prin urmare, elementele esențiale privind scopul sistemului, principiile de funcționare, subiecții, categoriile de date, condițiile de acces, validarea concordanței, jurnalizarea, auditul și garanțiile de protecție a datelor trebuie stabilite prin act normativ aprobat de Guvern, iar detaliile strict tehnice se reglementează prin documentația tehnică aferentă sistemului.

A patra opțiune analizată a vizat reglementarea integrală, prin prezenta hotărâre, inclusiv a tuturor mecanismelor de schimb automatizat transfrontalier. Această opțiune nu a fost reținută, deoarece componenta transfrontalieră depinde de intrarea în vigoare a legii speciale privind căutarea și schimbul automatizat de date în scopul cooperării polițienești și de îndeplinirea condițiilor juridice, organizatorice și tehnice necesare, inclusiv notificările, desemnarea punctelor de contact, actele de punere în aplicare și operaționalizarea mecanismelor externe aplicabile. Prin urmare, prezenta hotărâre trebuie să stabilească cadrul național de organizare și funcționare a SI RIF, iar aplicarea prevederilor privind schimbul transfrontalier să fie condiționată de cadrul legal special.

A cincea opțiune analizată a constat în includerea în hotărâre și în anexele acesteia a tuturor detaliilor tehnice privind arhitectura sistemului, algoritmii, interfețele, protocoalele, modelele de date și parametrii operaționali. Această opțiune nu a fost reținută, deoarece asemenea elemente au caracter tehnic și pot necesita actualizări periodice în funcție de evoluția infrastructurii, a cerințelor de securitate, a standardelor de interoperabilitate și a mecanismelor externe aplicabile. Proiectul stabilește nucleul normativ necesar, iar detaliile

tehnice urmează a fi reglementate prin documentația tehnică aferentă sistemului, aprobată în condițiile legii.

Ca urmare a analizei opțiunilor menționate, a fost reținută soluția instituirii Sistemului informațional „Registrul imaginilor faciale" ca sistem informațional distinct și specializat, cu aprobarea concomitentă a Conceptului și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale. Această soluție permite stabilirea unui cadru normativ clar, coerent și proporțional, asigurând delimitarea funcțională dintre componenta națională și setul de date destinat schimbului transfrontalier, protecția datelor cu caracter personal, controlul accesului, validarea umană a concordanței, jurnalizarea, auditul, securitatea informațională și interoperabilitatea cu sistemele informaționale relevante ale statului.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Proiectul va avea un impact direct asupra sectorului public, în special asupra autorităților și instituțiilor cu atribuții în domeniul ordinii și securității publice, prevenirii, constatării și investigării infracțiunilor, identificării persoanelor, căutării persoanelor dispărute, cooperării polițienești internaționale, administrării sistemelor informaționale, protecției datelor cu caracter personal și securității cibernetice.

Impactul principal constă în instituirea SI RIF ca resursă informațională specializată de stat cu destinație departamentală și în stabilirea cadrului normativ necesar pentru organizarea, administrarea, utilizarea, mentenanța și dezvoltarea acestuia. Proiectul stabilește Ministerul Afacerilor Interne în calitate de posesor al sistemului, cu responsabilitatea de a asigura condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea SI RIF.

Pentru Ministerul Afacerilor Interne, impactul va consta în consolidarea capacității instituționale de coordonare a proceselor aferente creării și utilizării RIF, inclusiv prin elaborarea actelor administrative subsecvente, stabilirea procedurilor interne, coordonarea autorităților participante, asigurarea guvernanței instituționale a sistemului și monitorizarea implementării cadrului normativ aprobat.

Pentru Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne, în calitate de deținător al SI RIF, impactul va consta în asumarea responsabilităților aferente creării, dezvoltării, mentenanței aplicative, funcționării tehnice a aplicației, administrării componentelor software, bazelor de date, interfețelor și mecanismelor aplicative de securitate, jurnalizare, monitorizare și audit, precum și asigurării suportului tehnic necesar funcționării sistemului, în limitele competențelor sale și în coordonare cu administratorul tehnic pentru aspectele ce țin de găzduire și infrastructura tehnologiilor informaționale.

Pentru Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică", în calitate de administrator tehnic al SI RIF, impactul va consta în asigurarea administrării tehnice a infrastructurii tehnologiilor informaționale aferente găzduirii SI RIF, mentenanței infrastructurii gestionate, măsurilor de securitate cibernetică și suportului tehnic aferent serviciilor prestate, în limitele competențelor stabilite de cadrul normativ aplicabil, fără intervenție în administrarea funcțională a datelor gestionate prin RIF.

Pentru autoritățile și instituțiile care vor avea calitatea de registratori, furnizori de date sau destinatari ai datelor, proiectul va genera obligații de ordin organizatoric și operațional, inclusiv desemnarea persoanelor autorizate, stabilirea rolurilor și profilurilor de acces, respectarea condițiilor de introducere, actualizare, rectificare, blocare, radiere și arhivare a datelor, respectarea procedurilor de comparare automatizată și validare a concordanțelor, precum și respectarea regulilor de jurnalizare, trasabilitate și securitate.

Impactul asupra sectorului public va fi pozitiv prin faptul că proiectul instituie un mecanism unitar, reglementat și controlabil de evidență și utilizare a imaginilor faciale. Acest lucru va permite autorităților competente să utilizeze datele într-un mod sigur și trasabil, reducând riscul prelucrărilor neuniforme, al accesului neautorizat la date sau al utilizării datelor în afara scopurilor prevăzute de lege.

Totodată, proiectul va contribui la creșterea capacității autorităților publice de a utiliza instrumente moderne în procesele de identificare ori verificare a identității persoanelor

bănuite, învinuite și condamnate, căutare a persoanelor dispărute, identificare a cadavrelor ori a părților acestora și sprijinire a activităților de prevenire, constatare și investigare a infracțiunilor. Acest impact va fi realizat cu respectarea garanțiilor privind legalitatea, proporționalitatea, limitarea scopului, validarea umană a concordanței, jurnalizarea și auditul operațiunilor.

Un impact relevant asupra sectorului public derivă și din necesitatea interoperabilității SI RIF cu alte sisteme informaționale și resurse informaționale relevante ale statului. Proiectul prevede interacțiunea prin MConnect, inclusiv, după caz, prin MConnect Events, precum și utilizarea serviciilor electronice guvernamentale partajate MCloud, MPass, MSign, MLog, MNotify și MPower, după caz. Aceasta va impune coordonare interinstituțională, definirea fluxurilor de date, stabilirea interfețelor tehnice și asigurarea compatibilității juridice, organizaționale, semantice și tehnice.

Proiectul nu implică crearea unei autorități publice noi și nu presupune modificarea structurii instituționale de bază a autorităților participante. Impactul este preponderent funcțional, organizatoric și tehnologic, fiind orientat spre instituirea unui cadru normativ clar pentru utilizarea unei resurse informaționale specializate și pentru delimitarea competențelor între proprietar, posesor, deținător, administrator tehnic, registratori, furnizori de date, destinatari ai datelor și utilizatori autorizați.

Implementarea proiectului va necesita pregătirea personalului implicat, elaborarea procedurilor operaționale, instruirea utilizatorilor autorizați și a personalului calificat implicat în validarea concordanțelor, stabilirea mecanismelor de control intern, aplicarea măsurilor de securitate informațională și cibernetică, realizarea evaluării impactului asupra protecției datelor cu caracter personal, precum și asigurarea auditului și monitorizării continue a utilizării sistemului.

În ceea ce privește componenta transfrontalieră, impactul asupra sectorului public va fi etapizat. Prevederile privind constituirea, utilizarea și schimbul automatizat transfrontalier al setului de date de referință privind imaginile faciale nu vor deveni aplicabile imediat, ci doar în condițiile stabilite în proiect, respectiv după intrarea în vigoare a legii speciale privind căutarea și schimbul automatizat de date în scopul cooperării polițienești și după îndeplinirea condițiilor juridice, organizatorice și tehnice necesare. Această abordare reduce riscul unei aplicări premature și permite autorităților publice să pregătească treptat cadrul instituțional, operațional și tehnic necesar.

Prin urmare, impactul asupra sectorului public este necesar și proporțional cu scopul urmărit. Proiectul va consolida capacitățile instituționale ale autorităților competente, va îmbunătăți guvernanța datelor biometrice faciale, va asigura trasabilitatea și controlul operațiunilor efectuate asupra datelor și va crea premisele pentru alinierea graduală la mecanismele europene de schimb automatizat de date în scopul cooperării polițienești.

4.2. Impactul financiar și argumentarea costurilor estimative

Implementarea proiectului va genera impact financiar asupra bugetului Ministerului Afacerilor Interne, determinat de necesitatea creării, dezvoltării, administrării, mentenanței și asigurării funcționării SI RIF. Proiectul prevede expres că Ministerul Afacerilor Interne, în calitate de posesor al SI RIF, va asigura condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea sistemului.

La etapa actuală, proiectul hotărârii Guvernului instituie cadrul normativ general pentru crearea și funcționarea SI RIF și nu stabilește alocări bugetare și obligații financiare imediate exprimate în sume fixe. Costurile efective vor putea fi determinate la etapa elaborării documentației tehnice, a specificațiilor funcționale și nefuncționale, a arhitecturii tehnologice, a cerințelor de interoperabilitate și securitate, precum și a planului de implementare.

Costurile aferente implementării SI RIF vor viza, în principal:

a) elaborarea și aprobarea documentației tehnice aferente sistemului;

b) dezvoltarea sau achiziționarea soluției informatice necesare funcționării SI RIF;

c) implementarea componentelor de recepționare, administrare, comparare biometrică facială, validare a concordanței, jurnalizare, audit și interoperabilitate;

d) integrarea cu sistemele informaționale și resursele informaționale relevante ale statului, inclusiv, după caz, prin MConnect, MPass, MLog, MSign, MNotify și MCloud;

e) asigurarea cerințelor de securitate informațională și securitate cibernetică;

f) configurarea rolurilor, profilurilor de acces, mecanismelor de autentificare și jurnalizare;

g) instruirea utilizatorilor autorizați și a personalului calificat implicat în validarea concordanțelor;

h) mentenanța, suportul tehnic, actualizarea și dezvoltarea ulterioară a sistemului.

Componenta privind schimbul automatizat transfrontalier al setului de date de referință privind imaginile faciale va putea genera costuri suplimentare distincte, aferente conectării la infrastructuri și mecanisme externe, configurării interfețelor tehnice, asigurării cerințelor de securitate și interoperabilitate, efectuării testărilor tehnice, precum și implementării actelor de punere în aplicare aplicabile. Aceste costuri urmează a fi determinate după intrarea în vigoare stabilirea condițiilor tehnice și aprobarea standardelor de către Comisia Europeană, clarificarea condițiilor juridice, organizatorice și tehnice necesare operaționalizării schimbului transfrontalier.

Finanțarea măsurilor de implementare va fi realizată în limita alocațiilor aprobate Ministerului Afacerilor Interne și instituțiilor din subordine, precum și, după caz, din alte surse legal disponibile, inclusiv proiecte de asistență externă, programe de suport tehnic sau alte mecanisme financiare aferente procesului de modernizare instituțională și integrare europeană.

Astfel, *proiectul nu instituie cheltuieli imediate prin aprobarea prezentului proiect de hotărâre, însă creează cadrul normativ care va permite planificarea etapizată a resurselor financiare necesare pentru dezvoltarea și funcționarea SI RIF*. Costurile vor fi justificate prin necesitatea instituirii unei resurse informaționale specializate de stat, capabile să asigure evidența, administrarea, compararea, validarea și utilizarea imaginilor faciale în condiții de legalitate, securitate, trasabilitate și interoperabilitate.

4.3. Impactul asupra sectorului privat

Proiectul nu instituie obligații directe pentru sectorul privat și nu stabilește sarcini administrative, financiare sau de raportare în privința persoanelor juridice de drept privat. Reglementările propuse vizează, în principal, instituirea și funcționarea unei resurse informaționale specializate de stat, gestionată în cadrul sectorului public, cu participarea autorităților și instituțiilor competente în domeniul ordinii și securității publice, prevenirii și investigării infracțiunilor, identificării persoanelor, interoperabilității și securității informaționale.

De asemenea, proiectul nu instituie obligații de furnizare a datelor de către entități private și nu creează cerințe noi de conformare pentru mediul de afaceri.

Impactul asupra sectorului privat poate fi unul indirect și limitat, în măsura în care, la etapa implementării tehnice a SI RIF, vor fi contractate servicii, lucrări sau produse din domeniul tehnologiei informației, securității cibernetice, interoperabilității, mentenanței, auditului tehnic sau instruirii. În asemenea cazuri, participarea operatorilor economici se va realiza în condițiile legislației privind achizițiile publice și ale contractelor încheiate cu autoritățile competente.

4.4. Impactul social

Proiectul va avea un impact social relevant, în special prin consolidarea capacităților autorităților competente de prevenire, constatare și investigare a infracțiunilor, identificare ori verificare a identității persoanelor, căutare a persoanelor dispărute și identificare a cadavrelor ori a părților acestora. Prin instituirea SI RIF, autoritățile publice vor dispune de un instrument specializat, reglementat și controlabil pentru gestionarea imaginilor faciale în condiții de legalitate, securitate, trasabilitate și protecție a datelor.

Impactul social pozitiv se va manifesta prin creșterea capacității statului de a reacționa mai eficient în cazurile ce implică identificarea persoanelor, inclusiv în cauze penale, cazuri de persoane dispărute, identificarea victimelor sau a cadavrelor ori a părților acestora. În acest sens, proiectul poate contribui la protejarea vieții, integrității și securității persoanelor, la sprijinirea victimelor și a familiilor persoanelor dispărute, precum și la îmbunătățirea activității autorităților responsabile de ordinea și securitatea publică.

Totodată, proiectul poate contribui la creșterea nivelului general de siguranță în societate, prin dezvoltarea unor mecanisme moderne de suport pentru activitățile de prevenire și combatere a criminalității.

În același timp, având în vedere că imaginile faciale reprezintă date biometrice și pot avea impact asupra vieții private și protecției datelor cu caracter personal, proiectul include garanții juridice și tehnice menite să limiteze riscurile sociale asociate utilizării unor asemenea date. Printre aceste garanții se regăsesc prelucrarea datelor numai în condițiile legii, limitarea scopului, accesul autorizat și diferențiat, interzicerea interogărilor generale, exploratorii sau nedeterminate, validarea umană a concordanței, jurnalizarea operațiunilor, trasabilitatea accesărilor, auditul și aplicarea măsurilor de securitate informațională.

4.4.1. Impactul asupra datelor cu caracter personal

Proiectul are un impact direct și semnificativ asupra domeniului protecției datelor cu caracter personal, întrucât SI RIF va gestiona imagini faciale, date de referință privind imaginile faciale, metadate aferente, rezultate ale comparării automatizate, liste ale mostrelor pentru care există posibilitatea unei concordanțe, precum și înregistrări privind confirmarea sau infirmarea concordanței. Prin natura lor, imaginile faciale utilizate pentru identificare biometrică reprezintă date cu caracter personal din perspectiva riscurilor asupra vieții private, identității persoanei și protecției împotriva accesului sau utilizării neautorizate.

Cadrul normativ aplicabil include Legea nr. 195/2024 privind protecția datelor cu caracter personal, legislația privind securitatea cibernetică, legislația privind schimbul de date și interoperabilitatea, actele normative privind resursele informaționale de stat și sistemele informaționale de stat, precum și normele speciale care reglementează activitatea autorităților competente. Proiectul include Legea nr. 195/2024 privind protecția datelor cu caracter personal, în cadrul normativ aplicabil creării, dezvoltării, administrării și funcționării SI RIF.

Impactul asupra datelor cu caracter personal se manifestă prin instituirea unei resurse informaționale specializate care va permite colectarea, recepționarea, introducerea, stocarea, actualizarea, rectificarea, blocarea, radierea, arhivarea, compararea automatizată, validarea concordanței, interoperabilitatea și, ulterior, schimbul automatizat transfrontalier al datelor de referință privind imaginile faciale. În acest sens, proiectul prevede că măsurile de securitate, jurnalizare, monitorizare, control și audit se aplică întregului ciclu de viață al datelor gestionate prin SI RIF.

Pentru diminuarea riscurilor asupra datelor cu caracter personal, proiectul instituie mai multe garanții juridice și tehnice. În primul rând, datele de referință privind imaginile faciale puse la dispoziție prin intermediul SI RIF nu conțin date suplimentare care permit identificarea directă a persoanei. Datele de identificare ale persoanei și alte informații suplimentare pot fi extrase și furnizate numai ulterior confirmării concordanței și numai în condițiile legii.

În al doilea rând, proiectul delimitează rezultatul tehnic preliminar al comparării automatizate de concordanța confirmată. Concordanța confirmată este definită ca o corespondență dintre două sau mai multe imagini faciale, stabilită în urma comparării automatizate și confirmată prin validare de către personal calificat. Lista mostrelor pentru care există posibilitatea unei concordanțe este calificată drept rezultat tehnic intermediar, care nu constituie concordanță confirmată și nu produce efecte juridice, procesuale, operaționale sau administrative până la validarea concordanței de către personal calificat.

În al treilea rând, proiectul instituie reguli privind accesul autorizat și diferențiat, jurnalizarea și trasabilitatea operațiunilor. Orice operațiune de introducere, actualizare, rectificare, completare, consultare, extragere, comparare, validare, transmitere, blocare, radiere sau arhivare a datelor din RIF se efectuează exclusiv în condițiile legii, în limita competențelor atribuite, cu asigurarea jurnalizării și trasabilității operațiunii efectuate, precum și a posibilității verificării și auditului utilizării datelor.

În al patrulea rând, proiectul reglementează securitatea informațională a SI RIF, inclusiv protecția datelor împotriva accesului, copierii, modificării, distrugerii, divulgării, transmiterii sau utilizării neautorizate. Măsurile tehnice și organizatorice prevăzute vizează autentificarea utilizatorilor, autorizarea și controlul accesului, confidențialitatea, integritatea și exactitatea

datelor, disponibilitatea și continuitatea funcționării, trasabilitatea operațiunilor, prevenirea incidentelor de securitate și recuperarea datelor în caz de incident, avarie sau dezastru.

Proiectul are impact și asupra schimbului de date prin interoperabilitate și, ulterior, asupra schimbului automatizat transfrontalier. Orice operațiune de consum, furnizare, transmitere sau recepționare a datelor prin interoperabilitate ori în cadrul schimbului automatizat transfrontalier urmează a fi înregistrată în evidențele SI RIF, astfel încât să permită identificarea utilizatorului sau a procesului tehnic, a datei și orei operațiunii, a temeiului operațiunii, a categoriei de date schimbate și a destinatarului ori sursei acestora.

Componenta transfrontalieră este reglementată într-o manieră etapizată și condiționată. Prevederile privind constituirea, utilizarea și schimbul automatizat transfrontalier al setului de date de referință privind imaginile faciale urmează a fi aplicate numai după intrarea în vigoare a actelor normative privind cooperarea polițienească internațională și după îndeplinirea condițiilor juridice, organizatorice și tehnice necesare. Această abordare reduce riscul prelucrării premature sau necorelate a datelor cu caracter personal în context transfrontalier.

Riscurile principale asociate proiectului privesc accesarea neautorizată a imaginilor faciale, utilizarea datelor în alte scopuri decât cele prevăzute de lege, corelarea excesivă a datelor, utilizarea eronată a rezultatului comparării automatizate, divulgarea neautorizată a datelor, compromiterea jurnalelor de acces sau producerea unor incidente de securitate. Aceste riscuri sunt diminuate prin limitarea scopurilor de prelucrare, separarea componentei naționale de setul de date de referință destinat schimbului transfrontalier, excluderea identificării directe pe baza datelor de referință, validarea umană a concordanței, controlul accesului, jurnalizarea, auditul, trasabilitatea și aplicarea măsurilor de securitate informațională și cibernetică.

Înainte de punerea în exploatare a SI RIF și, după caz, înainte de operaționalizarea componentei de schimb automatizat transfrontalier, posesorul sistemului urmează să asigure efectuarea evaluării impactului asupra protecției datelor cu caracter personal, în condițiile Legii nr. 195/2024, precum și implementarea măsurilor de diminuare a riscurilor identificate. Această măsură este necesară având în vedere natura biometrică a datelor prelucrate și potențialul impact asupra drepturilor și libertăților persoanelor vizate.

Prin urmare, proiectul comportă un impact asupra datelor cu caracter personal, dar include un set de garanții normative, organizatorice și tehnice destinate să asigure prelucrarea datelor în condiții de legalitate, necesitate, proporționalitate, securitate și trasabilitate. Implementarea SI RIF va necesita respectarea strictă a legislației privind protecția datelor cu caracter personal, realizarea măsurilor de securitate prevăzute de cadrul normativ aplicabil, instruirea utilizatorilor autorizați, controlul periodic al accesului și auditarea operațiunilor efectuate în sistem.

4.4.2. Impactul asupra echității și egalității de gen

Proiectul în cauză nu va avea impact asupra echității și egalității de gen.

4.5. Impactul asupra mediului

Proiectul în cauză nu va avea impact asupra mediului.

4.6. Alte impacturi și informații relevante

Proiectul în cauză nu va avea alte impacturi.

5. Compatibilitatea proiectului actului normativ cu legislația UE

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

Prezentul proiect reprezintă o măsură normativă necesară pentru transpunerea și implementarea în legislația națională a prevederilor 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 (Regulamentul Prüm II), act care stabilește cadrul pentru căutarea automatizată a profilurilor ADN, a datelor dactiloscopice, a imaginilor faciale, a evidențelor poliției și a anumitor date privind înmatricularea vehiculelor și care modifică Deciziile 2008/615/JAI și 2008/616/JAI. Regulamentul urmărește îmbunătățirea, simplificarea și facilitarea schimbului de date pentru cooperarea polițienească,

inclusiv prin extinderea schimburilor automatizate a datelor de referință privind imaginile faciale.

Prin proiect se asigură transpunerea parțială a cadrului juridic al Uniunii Europene aferent schimbului automatizat de date privind imaginile faciale, în special în partea ce ține de organizarea, ținerea și funcționarea resursei informaționale naționale privind imaginile faciale, constituirea datelor de referință privind imaginile faciale, excluderea datelor care permit identificarea directă a persoanei din setul de date de referință, utilizarea numerelor de referință, stabilirea componentelor funcționale necesare căutării automatizate, reglementarea răspunsurilor la solicitările de căutare automatizată, validarea umană a concordanțelor și asigurarea securității și trasabilității operațiunilor.

În concret, proiectul indică transpunerea parțială a art. 19, art. 20, art. 21, art. 22 alin. (1), art. 24 alin. (1) și (2) din Regulamentul (UE) 2024/982, în partea referitoare la imaginile faciale. Această transpunere se realizează prin aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale" și Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale.

Proiectul contribuie la transpunerea cerințelor UE prin instituirea unei resurse informaționale specializate care permite gestionarea imaginilor faciale în mod distinct, atribuirea numerelor de referință, delimitarea datelor de referință de datele de identificare directă, validarea umană a concordanței și asigurarea jurnalizării, trasabilității și securității prelucrărilor. Aceste elemente sunt necesare pentru crearea cadrului național de aplicare a mecanismelor de căutare și schimb automatizat de date privind imaginile faciale.

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

Proiectul hotărârii Guvernului urmărește crearea cadrului juridic intern necesar pentru implementarea, la nivel național, a prevederilor Regulamentului (UE) 2024/982 în partea referitoare la imaginile faciale, prin instituirea Sistemului informațional „Registrul imaginilor faciale" și aprobarea actelor normative subsecvente care reglementează organizarea și funcționarea acestuia.

Prin proiect se instituie SI RIF ca sistem informațional distinct și specializat, destinat formării, administrării, utilizării și, ulterior, schimbului automatizat al datelor de referință privind imaginile faciale, în condițiile cadrului normativ aplicabil cooperării polițienești internaționale și tratatelor internaționale. Proiectul aprobă Conceptul SI RIF și Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale, acestea constituind cadrul normativ secundar necesar pentru organizarea, dezvoltarea, administrarea și utilizarea sistemului.

Totodată, proiectul creează cadrul juridic intern pentru interoperabilitatea SI RIF cu sistemele informaționale și resursele informaționale relevante ale statului, prin intermediul MConnect și, după caz, al MConnect Events, precum și pentru utilizarea serviciilor electronice guvernamentale partajate relevante. Interacțiunea cu sistemele informaționale externe utilizate în cooperarea polițienească internațională va avea loc numai în condițiile actului normativ privind cooperarea polițienească internațională, ale tratatelor internaționale și ale actelor de punere în aplicare aplicabile.

6. Avizarea și consultarea publică a proiectului actului normativ

În scopul respectării prevederilor Legii nr. 239/2008 privind transparența în procesul decizional şi Regulamentului cu privire la procedurile de consultare publică cu societatea civilă în procesul decizional, aprobat prin Hotărârea Guvernului nr. 967/2016, anunțul de inițiere a elaborării proiectului a fost plasat pe platforma guvernamentală www.particip.gov.md

https://particip.gov.md/ro/document/stages/proiectul-hotararii-guvernului-cu-privire-la-aprobarea-conceptului-sistemului-informational-registr/16701

Este de menționat că, conform pct. 22 din Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, proiectul de hotărâre a fost examinat prealabil de către Agenția de Guvernare Electronică, iar propunerile și obiecțiile formulate (aviz nr.

3007-135 din 28 mai 2026) au fost integrate la definitivarea proiectului și reflectate în tabelul de sinteză.

Lista autorităților și instituțiilor care urmează să participe la avizarea proiectului:

1. Ministerul Justiției (inclusiv Administrația Națională a Penitenciarelor și Inspectoratul Național de Probațiune)
2. Ministerul Finanțelor (inclusiv Serviciul Vamal și Serviciul Fiscal de Stat);
3. Ministerul Dezvoltării Economice și Digitalizării;
4. Agenția de Guvernare Electronică;
5. Centrul Național pentru Protecția Datelor cu Caracter Personal;
6. Agenția Servicii Publice;
7. Procuratura Generală;
8. Serviciul de Informații și Securitate;
9. Serviciul Tehnologia Informației și Securitate Cibernetică.

Expertize:

1. Ministerul Justiției;
2. Centrul Național Anticorupție;
3. Centrul de Armonizare a Legislației

7. Concluziile expertizelor

Proiectul urmează a fi supus expertizei juridice, expertizei anticorupție și expertizei de compatibilitate cu legislația UE, în conformitate cu prevederile Legii nr. 100/2017 cu privire la actele normative.

8. Modul de încorporare a actului în cadrul normativ existent

Proiectul de hotărâre se încadrează în cadrul normativ și aprobarea acestuia nu necesită modificarea altor acte normative.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Implementarea proiectului va necesita măsuri juridice, organizatorice, tehnice și financiare pentru crearea, dezvoltarea, administrarea și utilizarea SI RIF. Ministerul Afacerilor Interne, în calitate de posesor al sistemului, va coordona procesul de implementare. Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne, în calitate de deținător al SI RIF, va asigura crearea, dezvoltarea, mentenanța aplicativă, funcționarea tehnică a aplicației, administrarea componentelor software, bazelor de date, interfețelor și mecanismelor aplicative de securitate, jurnalizare, monitorizare și audit. Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, în calitate de administrator tehnic, va asigura administrarea tehnică a infrastructurii tehnologiilor informaționale aferente găzduirii SI RIF, în limitele competențelor stabilite de cadrul normativ aplicabil.

Principalele măsuri necesare includ elaborarea documentației tehnice, dezvoltarea sau achiziționarea soluției informatice, integrarea cu sistemele informaționale relevante și cu serviciile electronice guvernamentale partajate, inclusiv MConnect și, după caz, MConnect Events, desemnarea utilizatorilor autorizați, aprobarea procedurilor de introducere, actualizare, comparare și validare a datelor, instruirea personalului, realizarea evaluării impactului asupra protecției datelor cu caracter personal, aplicarea măsurilor de protecție a datelor și securitate cibernetică, precum și testarea funcțională și de securitate a sistemului.

Componenta privind schimbul automatizat transfrontalier va fi implementată etapizat, numai după intrarea în vigoare actului normativ privind cooperarea polițienească internațională și după îndeplinirea condițiilor juridice, organizatorice și tehnice necesare, inclusiv efectuarea notificărilor, desemnarea punctelor de contact, aprobarea sau aplicarea actelor de punere în aplicare relevante și operaționalizarea mecanismelor externe aplicabile.

Secretar general al ministerului **Valentin CIOCLEA**

TABEL DE CONCORDANȚĂ

la proiectul hotărârii Guvernului cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale

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:** proiectul hotărârii Guvernului cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale
3.	**Gradul general de compatibilitate** Parțial compatibil
4.	**Autoritatea/persoana responsabilă** Ministerul Afacerilor Interne/ Vitalie Railean, șef al Secției politici în domeniul ordinii și securității publice
5.	**Data întocmirii/actualizării** 09.06.2026

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 „cadrul 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***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 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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) *autoritate competentă* – autoritate publică, instituție sau altă entitate abilitată prin lege să exercite atribuții în domeniile reglementate de prezenta lege. 2) *autoritate competentă de aplicare a legii* – 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) *autoritate de supraveghere* – 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) *baze de date INTERPOL* – 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) *Biroul Național SIRENE* - 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) *blocare de date* – marcarea prin acoperire a datelor cu caracter personal stocate, cu scopul de a limita prelucrarea lor ulterioară; 8) *cerere de informații* - 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) *concordanță (hit)* – 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) *date alfanumerice* – date constând în litere, cifre, caractere speciale, spații și semne de punctuație; 11) *date Europol* – orice date operaționale cu caracter personal prelucrate de Europol, statele membre și statele partenere, în conformitate cu mandatul Europol; 12) *date Interpol* – 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 acesteia privind prelucrarea datelor;

			13) *date de referință privind imaginea facială* – 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) *EPRIS* - 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) *EUCARIS* - Sistemul de informații european privind vehiculele și permisele de conducere; 16) *eveniment major cu dimensiune transfrontalieră* - 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) *evidențe ale poliției* – date biografice ale bănuiților, învinuiților, inculpaților și condamnaților, disponibile în bazele de date naționale instituite în scopul prevenirii, depistării și investigării infracțiunilor; 18) *informații* - 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 infracțiunilor, inclusiv informații operaționale în materie penală; 19) *imagine facială* – imagine digitală a feței unei persoane; 20) *imagine facială identificată* – imaginea facială a unei persoane identificate; 21) *imagine facială neidentificată* – imagine facială colectată în cadrul prevenirii, constatării sau investigării unei infracțiuni ori în cadrul căutării unei persoane dispărute fără veste sau al identificării cadavrelor sau părților acestuia, care nu este

			asociată, la momentul introducerii, unei persoane identificate; 22) *procedura de căutare automatizată* – 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*). 23) *punct național de contact* - 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) *punct unic de contact* - 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) *router* - 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) *SIENA* (acronim pentru *Secure Information Exchange Network Application*) – 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) *Sistemul de Informații Schengen (SIS)* – sistemul informatic centralizat, de scară largă, destinat cooperării polițienești și al cooperării judiciare în materie penală, controlului la trecerea frontierelor și returnărilor; 28) *SLTD (acronim pentru Stolen and Lost Travel Documents)* – 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) *stat solicitant* – statul care formulează o cerere de informații în sensul prezentei legi; 30) *stat solicitat* – statul căruia îi este adresată o cerere de informații în sensul prezentei legi; 31) *stat participant* – 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) *suspect* – persoana în privința căreia există motive serioase să se creadă că a săvârșit sau că urmează să săvârșească o infracțiune; 33) *sistem de schimb automatizat de date* – 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.			*profil ADN neidentificat* – 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*** *date dactiloscopice* – imagini de amprente digitale, imagini de amprente digitale latente, imagini de amprente palmare, imagini de amprente palmare latente, precum şi caracteristici codificate ale unor astfel de imagini stocate şi 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 *date dactiloscopice de referință* - 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 *date dactiloscopice neidentificate* - 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 *date dactiloscopice identificate* - 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.*** *date biometrice* – 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*** *pseudonimizare* – 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	***Art. 4 din Legea nr. 195/2024 privind protecția datelor cu caracter personal*** *date cu caracter personal* – 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	***Art. 2 Legea nr. 48/2023 privind securitatea cibernetică*** *incident cibernetic* – 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	***Proiectul de lege privind cooperarea polițienească***

respectivul incident are un impact redus și este probabil să fie deja bine înțeles în ceea ce privește metoda sau tehnologia;			***internațională*** 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*** *amenințare cibernetică semnificativă* – 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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 conțin 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** prevede și completarea ***Legii nr. 235/2017 cu privire la înregistrarea genetică judiciară, noțiunea „numere de referință" se substituie cu noțiunea „date de referință".*** **Articolul 2.** Noțiuni principale *date de referință ADN* – 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 ***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***.
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 ***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***
(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 ***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.***

			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 ***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***. 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 netranspusă	Prevederea urmează a fi transpusă prin intermediul unui ***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. 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 ***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***.
(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 ***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***.

(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	***Proiectul de lege privind cooperarea polițienească internațională*** **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 ***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***.
(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.			***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***.
(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 ***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***.
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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***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 *date dactiloscopice de referință*– 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 ***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”***.
(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 ***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”. 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 ***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”***. 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 ***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”***.
(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).			***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”***.
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 ***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”***.
(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 ***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”***.

(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 ***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”***.
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	***Proiectul de lege privind cooperarea polițienească internațională*** **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 dposesorul 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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 bănuit, 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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 ***proiect de modificare a Regulamentului cu privire la registrul de stat al vehiculelor, aprobat prin Hotărârea de Guvern nr. 1047/1999***.
(2) Informațiile schimbate prin Eucaris se transmit într-o formă criptată.		Prevedere UE netranspusă	Prevederea urmează a fi transpusă prin intermediul unui ***proiect de modificare a Regulamentului cu privire la registrul de stat al vehiculelor, aprobat prin Hotărârea de Guvern nr. 1047/1999***.
(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 ***proiect de modificare a Regulamentului cu privire la registrul de stat al vehiculelor, aprobat prin***

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).			***Hotărârea de Guvern nr. 1047/1999***. 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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. Respectivele 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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 ***proiect de modificare a Regulamentului cu***

prelucrării datelor, operatorii de date au acces la înregistrări pentru automonitorizarea menționată la articolul 55.			***privire la registrul de stat al vehiculelor, aprobat prin Hotărârea de Guvern nr. 1047/1999***.
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.	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale" și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** Anexa nr. 1 – Conceptul SI RIF: 10. În cadrul SI RIF se disting, din punct de vedere funcțional și juridic: 10.1. componenta națională a Registrului imaginilor faciale, care cuprinde totalitatea imaginilor faciale, a metadatelor aferente, a informațiilor asociate, a rezultatelor comparării automatizate și a altor date necesare realizării atribuțiilor autorităților competente, în condițiile legii; 10.2. setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier, care reprezintă o submulțime distinctă a datelor gestionate prin SI RIF și care este constituit, păstrat, furnizat și utilizat exclusiv în condițiile legii și ale tratatelor internaționale aplicabile; 10.3. setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier se constituie numai pentru categoriile de persoane care au calitatea de bănuit, învinuit, inculpat, condamnat pentru săvârșirea infracțiunilor, precum și, după caz, ale victimei, în măsură în care cadrul normativ național permite acest lucru.	Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **Articolul 18.** Date de referință privind imaginile faciale (1) Autoritatea competentă de aplicare a legii asigură disponibilitatea datelor de referință privind imaginile faciale ale bănuiților, învinuiților, inculpaților, condamnaților, și, după caz, ale victimelor din baza de date națională, în măsura în care cadrul normativ național permite acest lucru.

	10.4. imaginile faciale aferente persoanelor dispărute fără veste, cadavrelor ori părților acestora pot fi gestionate în componenta națională a Registrului imaginilor faciale, în condițiile legii, exclusiv pentru realizarea atribuțiilor autorităților competente privind căutarea persoanelor dispărute și identificarea cadavrelor ori a părților acestora, fără a fi incluse în setul de date de referință destinat schimbului automatizat transfrontalier. Anexa nr. 2 – Regulamentul RIF: 55. Introducerea datelor în setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier se efectuează numai pentru categoriile de persoane prevăzute de lege și numai dacă sunt întrunite condițiile juridice, tehnice și organizatorice aplicabile. 56. Setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier se constituie numai din datele de referință privind imaginile faciale ale persoanelor care au calitatea de bănuit, învinuit sau inculpat, ale persoanelor condamnate pentru săvârșirea infracțiunilor, precum și, după caz, ale victimei, în măsură 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.	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** Anexa nr. 1 – Conceptul SI RIF:	Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **Articolul 18.** Date de referință privind imaginile faciale (2) Datele de referință privind imaginile faciale puse la dispoziție

	11. Datele de referință privind imaginile faciale puse la dispoziție prin intermediul SI RIF nu conțin date suplimentare care permit identificarea directă a persoanei. Datele de identificare ale persoanei și alte informații suplimentare pot fi extrase și furnizate numai ulterior confirmării concordanței și numai în condițiile legii. 12.2. date de referință privind imaginile faciale – imagine facială și numărul de referință aferent, utilizate pentru compararea și schimbul automatizat transfrontalier al datelor, fără a permite identificarea directă a persoanei. 61.3. date privind obiectul informațional „date de referință privind imaginea facială”: 61.3.5. alte metadate strict necesare pentru compararea și schimbul automatizat, fără a permite identificarea directă a persoanei. 62. Datele de referință privind imaginea facială puse la dispoziție prin intermediul SI RIF nu conțin date suplimentare care permit identificarea directă a persoanei.		de autoritatea competentă de aplicare a legii nu conțin date care permit identificarea directă a persoanei.
(3) Imaginile faciale neidentificate sunt recunoscute ca atare.	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** Anexa nr. 1 – Conceptul SI RIF: 8. În Registrul imaginilor faciale se introduc imagini faciale identificate și imagini faciale neidentificate, obținute din	Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **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

	surse autorizate, precum și datele de referință aferente acestora. Imaginile faciale neidentificate se marchează și se recunosc ca atare. 12.5. imagine facială neidentificată – imagine facială colectată în cursul prevenirii, constatării sau investigării unei infracțiuni ori în cadrul căutării unei persoane dispărute sau al identificării cadavrelor ori a unor părți ale acestora, care nu sunt asociate, la momentul introducerii, unei persoane identificate. Anexa nr. 2 – Regulamentul RIF: 50. Introducerea unei imagini faciale neidentificate în RIF se efectuează cu marcarea distinctă a acesteia ca imagine facială neidentificată, fără asocierea prematură cu identitatea unei persoane, și cu consemnarea contextului de colectare, a sursei, a cauzei sau situației în care a fost obținută, precum și a altor metadate relevante. 51. Imaginile faciale neidentificate se marchează distinct la introducerea în RIF și se recunosc ca atare pe întreaga durată a prelucrării, până la identificarea persoanei sau până la radierea ori arhivarea datelor, în condițiile legii.		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	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale" și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** Anexa nr. 1 – Conceptul SI RIF: 14. Obiectivele SI RIF sunt: 14.1. asigurarea unei evidențe electronice specializate a imaginilor faciale	Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **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

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.	identificate și neidentificate, precum și a metadatelor și informațiilor asociate acestora, în cadrul componentei naționale a registrului; 14.2. asigurarea comparării automatizate a imaginilor faciale și a formării rezultatului tehnic preliminar al comparării, inclusiv, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe ori a rezultatului privind inexistența unei concordanțe posibile; 14.3. asigurarea validării, în condițiile legii, a rezultatului tehnic preliminar al comparării automatizate și, după caz, a concordanțelor posibile rezultate din aceasta; 14.4. constituirea distinctă, în cadrul SI RIF, a setului de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier; 14.5. asigurarea disponibilității setului de date de referință privind imaginile faciale pentru schimbul automatizat cu autoritățile competente străine și, după caz, cu alte entități abilitate prin lege, exclusiv în condițiile cadrului normativ aplicabil; 14.6. asigurarea interoperabilității cu sistemele informaționale și resursele informaționale relevante ale statului, fără a substitui funcțiile de evidență primară ale acestora; 14.7. asigurarea trasabilității operațiunilor de prelucrare, a accesului autorizat și diferențiat, precum și a securității informației și protecției datelor cu caracter personal;		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.

	14.8. consolidarea capacităților naționale în domeniul prevenirii, constatării și investigării infracțiunilor, al identificării persoanelor și al cooperării polițienești internaționale. 16. Căutarea automatizată a datelor de referință privind imaginile faciale în componenta de schimb automatizat transfrontalier se efectuează exclusiv în cazuri individuale, în condițiile legii. Utilizarea datelor gestionate prin SI RIF pentru interogări generale, exploratorii, nedeterminate sau pentru crearea de profiluri discriminatorii este interzisă. Anexa nr. 2 – Regulamentul RIF: 56. Setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier se constituie numai din datele de referință privind imaginile faciale ale persoanelor care au calitatea de bănuit, învinuit sau inculpat, ale persoanelor condamnate pentru săvârșirea infracțiunilor, precum și, după caz, ale victimei, în măsură în care cadrul normativ național permite acest lucru. 87. Accesul utilizatorilor la funcționalitățile SI RIF se realizează prin mijloace de autentificare și control al accesului conforme cadrului normativ aplicabil și politicilor de securitate aprobate. 88. Dreptul de acces la datele din RIF nu are caracter permanent și se menține doar pe perioada existenței temeiului juridic și a necesității funcționale care au justificat acordarea acestuia.		

(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.	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale" și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** Anexa nr. 1 – Conceptul SI RIF: 12.7. concordanță confirmată – corespondență dintre două sau mai multe imagini faciale, stabilită în urma comparării automatizate și confirmată prin validare de către personal calificat, în condițiile legii; 12.8. caz individual – situație concretă, individualizată și documentată potrivit legii, legată de prevenirea, constatarea sau investigarea unei infracțiuni, de căutarea unei persoane dispărute ori de identificarea unor cadavre sau a părților acestora; 12.9. validarea concordanței – verificarea rezultatului comparării automatizate de către personal calificat, în condițiile legii; 12.10. listă a mostrelor pentru care există posibilitatea unei concordanțe – rezultat tehnic intermediar al comparării automatizate, format din una sau mai multe mostre comparative selectate de SI RIF în baza nivelului de asemănare determinat potrivit regulilor de procesare aplicabile, care nu constituie concordanță confirmată și nu produce efecte juridice, procesuale, operaționale sau administrative până la validarea concordanței de către personal calificat. 26. Componenta de comparare biometrică facială asigură compararea automatizată a imaginilor faciale cu datele comparative	Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **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.

	privind imaginile faciale disponibile, inclusiv prin mecanisme de tip 1:1 și 1:N, determinarea nivelului de asemănare, generarea rezultatului tehnic preliminar al comparării și, după caz, formarea listei mostrelor pentru care există posibilitatea unei concordanțe, fără ca nivelul de asemănare ori lista respectivă să constituie concordanță confirmată. 28. Componenta de validare a concordanței asigură verificarea de către personal calificat a rezultatului comparării automatizate și, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe, confirmarea sau infirmarea concordanței și înregistrarea rezultatului validării. Anexa nr. 2 – Regulamentul RIF: Secțiunea a 5-a Validarea concordanței 134. Validarea concordanței reprezintă verificarea umană a rezultatului comparării automatizate și, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe, de către personal calificat, în vederea confirmării, infirmării concordanței ori constatării unui rezultat neconcludent. 135. Validarea concordanței se efectuează numai de către personal calificat, desemnat prin act administrativ al autorității competente, care a urmat instruirea necesară pentru utilizarea SI RIF, interpretarea rezultatelor comparării biometrice faciale, aplicarea cerințelor de protecție a datelor și respectarea procedurilor de jurnalizare și trasabilitate.		

	136. Validarea concordanței este obligatorie în toate cazurile în care rezultatul comparării automatizate este utilizat pentru: 136.1. identificarea ori verificarea identității unei persoane; 136.2. individualizarea unui caz; 136.3. extragerea datelor de bază sau a informațiilor suplimentare; 136.4. furnizarea unor date în cadrul cooperării polițienești internaționale; 136.5. luarea unei măsuri operaționale ori procedurale care poate produce efecte juridice sau factuale relevante. 137. În procesul validării concordanței, personalul calificat examinează cel puțin: 137.1. imaginea facială supusă comparării; 137.2. mostra sau mostrele comparative indicate de sistem; 137.3. nivelul de asemănare și relevanța rezultatului tehnic; 137.4. calitatea imaginilor comparate; 137.5. contextul cazului individual; 137.6. existența unor elemente care pot conduce la confuzie, eroare sau concluzii neveridice. 138. În urma validării, rezultatul se consemnează ca: 138.1. concordanță confirmată; 138.2. concordanță infirmată; 138.3. rezultat neconcludent, atunci când datele disponibile nu permit o concluzie suficient de certă și sunt necesare verificări suplimentare.		

	139. În cazul în care autoritatea competentă a Republicii Moldova are calitatea de autoritate solicitată în cadrul schimbului automatizat transfrontalier, confirmarea concordanței se efectuează numai după revizuirea manuală a rezultatului comparării automatizate și, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe, de către cel puțin un membru calificat al personalului, în condițiile legii. 140. Confirmarea concordanței nu echivalează, prin ea însăși, cu stabilirea definitivă a identității persoanei în afara cadrului procedural aplicabil și nu substituie alte verificări, expertize sau acte procedurale cerute de lege. 141. În situația infirmării concordanței, rezultatul comparării nu poate fi utilizat ca temei pentru extragerea ori furnizarea datelor de bază și a informațiilor suplimentare, cu excepția păstrării sale în evidențele sistemului pentru trasabilitate, control și audit.		
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	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** Anexa nr. 1 – Conceptul SI RIF: 9. Fiecărei imagini faciale introduse în Registrul imaginilor faciale i se atribuie un număr de referință, utilizat ca identificator al obiectului informațional și ca element de legătură pentru extragerea, după caz, a datelor	Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **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

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.	de bază și a informațiilor suplimentare în cazul unei concordanțe confirmate. 12.6. număr de referință – identificator alfanumeric unic atribuit imaginii faciale, care include elementele tehnice prevăzute de lege și de documentația tehnică aplicabilă, inclusiv, după caz, codul statului, identificatorul unic al imaginii faciale și indicatorul privind caracterul identificat sau neidentificat al imaginii, fără a conține date care permit identificarea directă a persoanei; 57. Identificatorii principali utilizați în SI RIF sunt următorii: 57.1. pentru imaginea facială identificată – numărul de referință al imaginii faciale, identificatorul intern al înregistrării în SI RIF, precum și identificatorul persoanei fizice din sistemul-sursă, respectiv IDNP, după caz, sau alt identificator oficial atribuit în sistemul-sursă; 57.2. pentru imaginea facială neidentificată – numărul de referință al imaginii faciale, identificatorul intern al înregistrării în SI RIF, indicatorul caracterului neidentificat al imaginii faciale, precum și identificatorul cazului individual, al cauzei penale, al dosarului de căutare ori al altui obiect informațional conex din sistemul-sursă; 57.3. pentru datele de referință privind imaginea facială – numărul de referință și codurile asociate prevăzute de cadrul normativ aplicabil; 57.4. pentru solicitarea de căutare automatizată a datelor de referință privind imaginile faciale– numărul solicitării, data și ora solicitării, codul statului solicitant precum		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.

	și, datele de referință privind imaginile faciale; 57.5. pentru răspunsul la solicitarea de căutare automatizată a datelor de referință privind imaginile faciale – numărul răspunsului, data și ora răspunsului, precum și numărul solicitării la care acesta se referă; 57.6. pentru rezultatul comparării automatizate – identificatorul rezultatului comparării, numărul de referință al imaginii faciale supuse comparării și, după caz, numărul de referință al mostrei comparative; 57.7. pentru înregistrarea privind confirmarea sau infirmarea concordanței – identificatorul validării, identificatorul rezultatului comparării și datele privind statutul validării. 57.8. pentru obiectele informaționale împrumutate – identificatorii atribuiți acestora în sistemele informaționale și resursele informaționale-sursă, inclusiv IDNP pentru persoana fizică, IDNO pentru unitatea de drept și identificatorul cauzei penale, dosarului de căutare, cazului individual ori al altui obiect informațional conex, după caz. 61.3. date privind obiectul informațional „date de referință privind imaginea facială”: 61.3.1. imaginea facială; 61.3.2. numărul de referință; 61.3.3. codul statului care deține imaginea facială; 61.3.4. indicatorul care arată caracterul identificat sau neidentificat al imaginii faciale; 61.3.5. alte metadate strict necesare pentru compararea și schimbul automatizat,		

	fără a permite identificarea directă a persoanei. Anexa nr. 2 – Regulamentul RIF: 51. Imaginile faciale neidentificate se marchează distinct la introducerea în RIF și se recunosc ca atare pe întreaga durată a prelucrării, până la identificarea persoanei sau până la radierea ori arhivarea datelor, în condițiile legii. 52. Numărul de referință se atribuie la momentul introducerii în RIF și se utilizează ca identificator unic al obiectului informațional, inclusiv pentru corelarea acestuia cu datele de bază și informațiile suplimentare care pot fi extrase ulterior, în condițiile legii. 53. Numărul de referință este utilizat ca element de legătură pentru corelarea controlată cu metadatele, rezultatele comparării automatizate, înregistrările privind validarea concordanței și, după caz, datele de bază ori informațiile suplimentare care pot fi extrase ulterior, în condițiile legii.		
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.	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale" și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** Anexa nr. 1 – Conceptul SI RIF: 15.8. principiul securității informației, potrivit căruia datele sunt protejate prin măsuri tehnice și organizatorice adecvate, care asigură confidențialitatea, integritatea, disponibilitatea și reziliența sistemului;	Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **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

	15.9. principiul trasabilității, potrivit căruia toate operațiunile relevante efectuate în sistem sunt jurnalizate și pot fi verificate ulterior 31. Componenta de administrare, securitate, jurnalizare și audit asigură: 31.1. administrarea utilizatorilor, rolurilor și drepturilor de acces; 31.2. administrarea nomenclatoarelor și a metadatelor de sistem; 31.3. jurnalizarea operațiunilor efectuate în sistem; 31.4. monitorizarea utilizării sistemului; 31.5. aplicarea măsurilor tehnice și organizatorice de securitate; 31.6. auditul și trasabilitatea operațiunilor. 74. SI RIF este găzduit pe platforma tehnologică guvernamentală comună (MCloud) în conformitate cu Hotărârea Guvernului nr. 128/2014 cu privire la platforma tehnologică guvernamentală comună (MCloud), iar aspectele ce țin de găzduirea, administrarea tehnică a infrastructurii și securitatea cibernetică se coordonează cu Instituția publică ,,Serviciul Tehnologia Informației și Securitate Cibernetică”, potrivit cadrului normativ aplicabil. 75. Pentru schimbul de date și interoperabilitatea cu alte sisteme informaționale și resurse informaționale de stat, SI RIF interacționează prin intermediul platformei guvernamentale de interoperabilitate (MConnect), inclusiv după		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.

	caz, cu utilizarea componentei MConnect Events prin interfețe de programare a aplicațiilor (API), pentru expunerea și consumul evenimentelor de sistem relevante pentru interoperabilitate, în condițiile cadrului normativ aplicabil, a cerințelor tehnice stabilite de Instituția publică „Agenția de Guvernare Electronică”, ale cerințelor de securitate și ale documentației tehnice aferente SI RIF, precum și cu următoarele sisteme informaționale partajate: 75.1. serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea utilizatorilor și controlul accesului în cadrul sistemului; 75.2. serviciul electronic guvernamental integrat de semnătură electronică (MSign) – pentru semnarea documentelor electronice, după caz; 75.3. serviciul electronic guvernamental de jurnalizare (MLog) – pentru asigurarea evidenței operațiunilor și a trasabilității activităților desfășurate în sistem; 75.4. serviciul guvernamental de notificare electronică (MNotify) – pentru notificarea furnizorilor de date, registratorilor și utilizatorilor, după caz. Anexa nr. 2 – Regulamentul RIF: Capitolul VIII. Securitatea, jurnalizarea, monitorizarea, controlul și auditul Secțiunea 1 Dispoziții generale 179. Securitatea, jurnalizarea, monitorizarea, controlul și auditul în cadrul RIF se asigură în scopul garantării legalității		

	prelucrării datelor, al protejării confidențialității, integrității, disponibilității, autenticității și rezilienței SI RIF, al prevenirii accesului neautorizat, al detectării utilizărilor neconforme și al asigurării trasabilității complete a operațiunilor efectuate în sistem. 180. Măsurile de securitate, jurnalizare, monitorizare, control și audit prevăzute în prezentul capitol se aplică întregului ciclu de viață al datelor gestionate prin SI RIF, inclusiv la colectarea, recepționarea, introducerea, stocarea, actualizarea, rectificarea, blocarea, radierea, arhivarea, compararea automatizată, validarea concordanței, interoperabilitatea și schimbul de date. 181. Posesorul, deținătorul, administratorul tehnic, registratorii, furnizorii de date, destinatarii datelor și ceilalți utilizatori autorizați ai SI RIF au obligația să respecte cerințele de securitate, jurnalizare, monitorizare și audit stabilite de prezentul Regulament, de actele administrative aprobate în temeiul acestuia și de legislația aplicabilă în domeniul protecției datelor cu caracter personal și al securității cibernetice. 182. Posesorul aprobă procedurile interne privind securitatea, administrarea accesului, jurnalizarea, monitorizarea și auditul SI RIF, deținătorul asigură implementarea tehnică aplicativă a acestora, iar administratorul tehnic asigură măsurile tehnice aferente infrastructurii administrate, în limitele competențelor stabilite de lege. 183. Înainte de punerea în exploatare a SI RIF și, după caz, înainte de		

	operaționalizarea componentei de schimb automatizat transfrontalier, posesorul asigură evaluarea impactului asupra protecției datelor cu caracter personal, în condițiile Legii nr. 195/2024 privind protecția datelor cu caracter personal, precum și implementarea măsurilor de diminuare a riscurilor identificate. Secțiunea a 2-a Măsurile de securitate ale SI RIF 184. SI RIF se exploatează cu aplicarea unor măsuri tehnice și organizatorice adecvate pentru: 183.1. autentificarea utilizatorilor; 183.2. autorizarea și controlul accesului; 183.3. asigurarea confidențialității datelor; 183.4. asigurarea integrității și exactității datelor; 183.5. asigurarea disponibilității și continuității funcționării; 183.6. asigurarea autenticității și trasabilității operațiunilor; 183.7. prevenirea, detectarea și limitarea incidentelor de securitate; 183.8. restabilirea funcționării și recuperarea datelor în caz de incident, avarie sau dezastru. 185. Accesul la funcționalitățile SI RIF se realizează numai prin mecanisme de autentificare și control al accesului conforme cadrului normativ aplicabil și politicilor de securitate aprobate, inclusiv, după caz, prin utilizarea serviciilor guvernamentale comune destinate autentificării.		

	186. Datele gestionate prin SI RIF se protejează împotriva accesului, copierii, modificării, distrugerii, divulgării, transmiterii sau utilizării neautorizate, inclusiv prin măsuri de segmentare logică, separare a rolurilor, restricționare a privilegiilor, criptare, protecție a comunicațiilor și alte măsuri tehnice adecvate. 187. Componenta națională a RIF și setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier se protejează distinct, prin măsuri diferențiate de acces, utilizare, transmitere și administrare, corespunzător regimului juridic aplicabil fiecărei componente. 188. Găzduirea și exploatarea tehnologică a SI RIF se realizează prin utilizarea platformei tehnologice guvernamentale comune sau a altor infrastructuri permise de cadrul normativ aplicabil, cu respectarea cerințelor de securitate, continuitate operațională și reziliență. 189. Deținătorul asigură efectuarea copiilor de rezervă, menținerea mecanismelor de recuperare a datelor și aplicarea măsurilor de continuitate a funcționării și de restabilire a serviciilor în caz de incidente sau dezastre. 190. În cazul apariției unei amenințări cibernetice, a unui incident de securitate, a unei neconformități grave ori a unui risc iminent pentru legalitatea sau siguranța funcționării SI RIF, deținătorul poate restricționa sau suspenda temporar accesul tehnic la sistem ori la anumite		

	funcționalități ale acestuia, cu informarea imediată a posesorului și cu aplicarea măsurilor de remediere necesare. Secțiunea a 3-a Jurnalizarea operațiunilor 191. SI RIF asigură jurnalizarea automată a tuturor operațiunilor relevante efectuate în sistem, inclusiv a celor de autentificare, accesare, consultare, introducere, actualizare, rectificare, blocare, radiere, arhivare, comparare automatizată, validare a concordanței, extragere, furnizare, transmitere, recepționare, suspendare a accesului și administrare a conturilor ori profilurilor de acces. 192. Jurnalizarea trebuie să permită identificarea cel puțin a: 191.1. utilizatorului sau procesului tehnic care a efectuat operațiunea; 191.2. rolului și instituției de apartenență, după caz; 191.3. datei și orei operațiunii; 191.4. tipului operațiunii efectuate; 191.5. obiectului informațional vizat; 191.6. temeiului sau justificării operațiunii, în măsura în care aceasta este asociată unui caz individual ori unei sarcini concrete; 191.7. sursei sau destinatarului datelor, după caz; 191.8. rezultatului operațiunii. 193. Evidențele de jurnalizare se păstrează în condiții de securitate, separat de mediile operaționale, cu protecție împotriva		

	modificării, ștergerii, divulgării ori accesării neautorizate. 194. Jurnalele SI RIF pot fi ținute prin mecanisme interne ale sistemului și, după caz, prin utilizarea serviciilor guvernamentale comune de jurnalizare, în condițiile cadrului normativ aplicabil. 195. Accesul la jurnalele SI RIF este permis numai persoanelor expres autorizate în scop de administrare tehnică, securitate, control intern, audit, investigare a incidentelor, verificare a legalității prelucrării sau stabilire a răspunderii, în condițiile legii. 196. Modificarea, alterarea, ștergerea ori ascunderea neautorizată a înregistrărilor din jurnalele SI RIF este interzisă și atrage răspunderea prevăzută de lege. Secțiunea a 4-a Monitorizarea utilizării SI RIF 197. Monitorizarea SI RIF reprezintă activitatea continuă de supraveghere a funcționării tehnice, a utilizării operaționale și a respectării cerințelor de securitate și legalitate în procesul de prelucrare a datelor gestionate prin sistem. 198. Monitorizarea SI RIF are ca obiective: 197.1. verificarea funcționalității continue a sistemului; 197.2. identificarea accesărilor neautorizate sau neobișnuite; 197.3. detectarea incidentelor de securitate, a vulnerabilităților și a neconformităților;		

	197.4. verificarea respectării profilurilor de acces și a regulilor de utilizare; 197.5. examinarea frecventă a log-urilor și a activităților de prelucrare; 197.6. evaluarea necesității măsurilor de remediere, restricționare ori suspendare a accesului. 199. Posesorul monitorizează implementarea și funcționarea RIF, inclusiv pe componenta de schimb automatizat transfrontalier, iar deținătorul asigură monitorizarea tehnică permanentă a funcționalității sistemului și informează posesorul despre incidentele, deficiențele și riscurile identificate. 200. În cazul constatării unor utilizări neconforme, a unor accesări neautorizate, a unor incidente de securitate sau a altor neconformități, se dispun fără întârziere măsurile necesare pentru limitarea efectelor, remedierea cauzelor, conservarea probelor și, după caz, sesizarea autorităților competente. Secțiunea a 5-a Controlul intern și auditul 201. Controlul intern asupra utilizării SI RIF se exercită de către posesor și, după caz, de către alte structuri competente, în limitele atribuțiilor stabilite de lege și de actele administrative interne. 202. Controlul intern vizează, după caz: 201.1. legalitatea accesului și utilizării datelor;		

	201.2. respectarea profilurilor de acces și a separării rolurilor; 201.3. respectarea procedurilor privind introducerea, actualizarea, rectificarea, blocarea, radierea, compararea, validarea și schimbul de date; 201.4. respectarea cerințelor de securitate și confidențialitate; 201.5. respectarea obligațiilor de jurnalizare și păstrare a evidențelor; 201.6. conformitatea cu prezentul Regulament și cu actele administrative interne adoptate în executarea acestuia. 203. Auditul SI RIF se efectuează periodic sau ori de câte ori este necesar, în scopul evaluării conformității juridice, organizatorice și tehnice a funcționării sistemului, al verificării eficacității măsurilor de securitate și al identificării riscurilor și vulnerabilităților. 204. Auditul poate avea, după caz, caracter tehnic, de securitate, de conformitate, de protecție a datelor cu caracter personal ori mixt, în funcție de obiectul și necesitatea verificării. 205. În cadrul auditului, auditorii sau persoanele împuternicite pot avea acces, în limitele competențelor legale, la configurațiile tehnice, jurnalele sistemului, evidențele operațiunilor, documentele justificative, procedurile interne, registrele de acces, rapoartele de incident și alte materiale necesare verificării. 206. Rezultatele controlului și ale auditului se consemnează în acte de constatare, rapoarte ori alte documente		

	interne, care includ, după caz, neconformitățile identificate, riscurile constatate, măsurile de remediere recomandate, termenele de executare și subiecții responsabili. 207. Posesorul dispune măsurile de remediere necesare în urma constatărilor controlului sau auditului și monitorizează executarea acestora. Secțiunea a 6-a Gestionarea incidentelor și răspunderea 208. Orice utilizator, registrator, furnizor de date, destinatar al datelor, administrator tehnic ori alt subiect care constată un incident de securitate, o accesare neautorizată, o pierdere de date, o neconcordanță relevantă ori o utilizare neconformă a SI RIF este obligat să informeze fără întârziere deținătorul și posesorul, potrivit procedurilor interne aplicabile. 209. Gestionarea incidentelor de securitate include, după caz: 208.1. înregistrarea incidentului; 208.2. evaluarea naturii și gravității acestuia; 208.3. limitarea efectelor și izolarea componentelor afectate; 208.4. conservarea urmelor și a dovezilor digitale relevante; 208.5. remedierea cauzelor; 208.6. restabilirea funcționării; 208.7. informarea subiecților competenți și notificarea autorităților competente, în cazurile și condițiile prevăzute de lege.		

	210. În cazul incidentelor care afectează date cu caracter personal ori securitatea cibernetică, se aplică procedurile de notificare, cooperare și răspuns prevăzute de legislația specială aplicabilă. 211. Utilizarea abuzivă a datelor, accesarea neautorizată a SI RIF, încălcarea obligațiilor de confidențialitate, alterarea jurnalelor, nerespectarea măsurilor de securitate, precum și orice altă prelucrare neconformă a datelor gestionate prin SI RIF atrag răspunderea disciplinară, contravențională, civilă sau penală, după caz, potrivit legii. 212. Cerințele tehnice detaliate privind securitatea, jurnalizarea, monitorizarea, controlul, auditul, copiile de rezervă, continuitatea activității, recuperarea în caz de dezastru și gestionarea incidentelor se stabilesc prin documentația tehnică a SI RIF și prin actele administrative aprobate în temeiul prezentului Regulament.		
(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 revizuiește actele de punere în aplicare respective.	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** Anexa nr. 1 – Conceptul SI RIF: 33. SI RIF asigură funcționalități care permit: 33.1. utilizarea imaginilor faciale conforme cerințelor minime de calitate stabilite potrivit cadrului normativ aplicabil și documentației tehnice a sistemului, pentru compararea automatizată.	Parțial compatibil O parte din prevederea 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.

	69. Regulile de validare aplicabile datelor introduse și procesate în SI RIF asigură: 69.8. verificarea calității minime a imaginii faciale pentru utilizarea acesteia în compararea automatizată; Anexa nr. 2 – Regulamentul RIF: 47. Înainte de introducerea datelor în RIF, registratorul verifică: 47.5. calitatea suficientă a imaginii faciale pentru prelucrarea ulterioară, inclusiv pentru compararea automatizată, după caz;		Obligația națională de a transmite numai imagini de calitate suficientă a fost introdusă în proiectul de hotărâre ***cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale" și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale***, 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.	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale" și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** Anexa nr. 1 – Conceptul SI RIF: 33. SI RIF asigură funcționalități care permit: 33.1. utilizarea imaginilor faciale conforme cerințelor minime de calitate stabilite potrivit cadrului normativ aplicabil și documentației tehnice a sistemului, pentru compararea automatizată; 59. Identificatorii utilizați în SI RIF sunt aliniați la cerințele cadrului normativ național și, după caz, la standardele și cerințele tehnice internaționale aplicabile, astfel încât să fie asigurată interoperabilitatea cu alte sisteme informaționale de stat și cu infrastructurile externe utilizate în cooperarea polițienească internațională.	Parțial compatibil O parte din prevedere UE este neaplicabilă se referă la activitatea Comisiei	***Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale" și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale*** prevede expres că digitalizarea, transmiterea și compararea imaginilor faciale se fac conform standardelor europene sau internaționale relevante. În schimb, dispoziția privind 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

	64. Structura tehnică detaliată a atributelor obiectelor informaționale gestionate în SI RIF, precum și regulile tehnice de completare, validare, actualizare și corelare automată a acestora se stabilesc prin documentația tehnică aferentă sistemului. 73. Structura și conținutul nomenclatoarelor, clasificatoarelor, tabelelor de coduri și regulilor de validare, precum și modul de administrare și actualizare a acestora se stabilesc prin documentația tehnică aferentă sistemului.		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 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	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** Anexa nr. 1 – Conceptul SI RIF: 30. Componenta de interoperabilitate cu sistemele informaționale externe utilizate în cooperarea polițienească internațională asigură, în condițiile legii speciale privind	Parțial compatibil	Capacitățile maxime de căutare, procedura de majorare temporară/permanentă și fluxul de notificare urmează a fi stabilite la etapa operaționalizării schimbului automatizat transfrontalier, în corelare cu legea specială privind cooperarea polițienească internațională, actele de punere în

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.	cooperarea polițienească internațională, ale tratatelor internaționale și ale actelor de punere în aplicare aplicabile, constituirea, extragerea, furnizarea, recepționarea și schimbul automatizat al setului de date de referință privind imaginile faciale, transmiterea și recepționarea solicitărilor și răspunsurilor de căutare automatizată, precum și suportul tehnic pentru furnizarea ulterioară a datelor de bază și a informațiilor suplimentare numai după confirmarea concordanței. 33. SI RIF asigură funcționalități care permit: 33.1. utilizarea imaginilor faciale conforme cerințelor minime de calitate stabilite potrivit cadrului normativ aplicabil și documentației tehnice a sistemului, pentru compararea automatizată; 33.2. delimitarea funcțională dintre componenta națională a registrului și setul de date de referință destinat schimbului automatizat transfrontalier; 33.3. limitarea schimbului automatizat la setul de date strict necesar; 33.4. utilizarea numerelor de referință; 33.5. păstrarea istoricului actualizărilor și a rezultatelor comparării; 33.6. utilizarea componentei de schimb automatizat transfrontalier numai în cazuri individuale; 33.7. prevenirea accesului neautorizat și a utilizării datelor în scopuri incompatibile cu cadrul normativ aplicabil și cu scopurile pentru care SI RIF a fost instituit.		aplicare ale UE și documentația tehnică aferentă SI RIF.

	111. Soluțiile tehnice utilizate în cadrul SI RIF permit implementarea funcționalităților prevăzute de cadrul normativ național și de actele Uniunii Europene relevante pentru căutarea și schimbul automatizat de date în scopul cooperării polițienești, în partea referitoare la imaginile faciale, inclusiv cerințele privind datele de referință, solicitările și răspunsurile automatizate și utilizarea în cazuri individuale prevăzute de Regulamentul (UE) 2024/982. 112. Structura detaliată a componentelor informaționale și tehnologice, cerințele funcționale și nefuncționale, mecanismele de integrare, modelele de date, protocoalele de schimb și condițiile de administrare tehnică se stabilesc prin documentația tehnică aferentă sistemului, iar măsurile generale de securitate se stabilesc prin Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale și prin actele normative aplicabile.		
(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).		Prevedere UE neaplicabilă	Dispoziția conferă Comisiei Europene competența de a adopta acte de punere în aplicare privind numărul maxim de candidați acceptați pentru comparație și distribuția capacităților de căutare nefolosite. Această competență ține de cadrul instituțional al Uniunii Europene și nu se transpune în actul normativ național. Proiectul hotărârii poate prevedea doar conformarea tehnică la parametrii stabiliți la nivelul UE.

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.	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** Anexa nr. 1 – Conceptul SI RIF: 61.4. date privind obiectul informațional „solicitarea de căutare automatizată a datelor de referință privind imaginile faciale”: 61.4.1. codul statului solicitant; 61.4.2. data solicitării; 61.4.3. ora solicitării; 61.4.4. numărul solicitării; 61.4.5. datele de referință privind imaginea facială.	Compatibil	
(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; (f) imaginile faciale între care s-a stabilit o concordanță.	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** Anexa nr. 1 – Conceptul SI RIF: 61.5. date privind obiectul informațional „răspunsul la solicitarea de căutare automatizată a datelor de referință privind imaginile faciale”: 61.5.1. mențiunea existenței unei concordanțe, a mai multor concordanțe sau a inexistenței concordanței; 61.5.2. data solicitării; 61.5.3. ora solicitării; 61.5.4. numărul solicitării; 61.5.5. data răspunsului; 61.5.6. ora răspunsului;	Compatibil	

	61.5.7. numărul răspunsului; 61.5.8. codul statului solicitant; 61.5.9. codul statului solicitat; 61.5.10. numerele de referință ale imaginilor faciale din statul solicitant și din statul solicitat; 61.5.11. 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.	**Proiectul HG cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale" și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale** 4. Prevederile prezentei hotărâri referitoare la constituirea, utilizarea și schimbul automatizat transfrontalier al setului de date de referință privind imaginile faciale se aplică de la data intrării în vigoare a legii speciale privind cooperarea polițienească internațională și după îndeplinirea condițiilor juridice, organizatorice și tehnice prevăzute de aceasta, inclusiv efectuarea notificărilor, desemnarea punctelor de contact și operaționalizarea mecanismelor externe aplicabile. Anexa nr. 2 – Regulamentul RIF: 24. Posesorul SI RIF are obligația: 24.5. să asigure, prin intermediul mecanismelor prevăzute de lege, notificarea și actualizarea informațiilor privind conținutul bazei de date naționale privind imaginile faciale, condițiile tehnice și juridice ale căutărilor automatizate, lista autorităților autorizate și profilurile de acces ale personalului autorizat.	Parțial compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **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

	164. Funcționalitățile aferente schimbului automatizat transfrontalier al datelor de referință privind imaginile faciale se pun în aplicare numai după asigurarea condițiilor juridice, organizatorice și tehnice necesare, inclusiv, după caz, a notificărilor, desemnărilor și actelor de punere în aplicare prevăzute de lege.		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. Proiectul hotărârii Guvernului condiționează aplicarea prevederilor privind constituirea, utilizarea și schimbul automatizat transfrontalier al setului de date de referință de intrarea în vigoare a legii speciale privind cooperarea polițienească internațională și de asigurarea condițiilor juridice, organizatorice și tehnice necesare, inclusiv notificările, actele de punere în aplicare și operaționalizarea mecanismelor externe aplicabile.
Articolul 25. Evidențe ale poliției (1) Statele membre pot participa la schimbul automatizat de evidențe ale poliției.		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională***

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 suspecților și ale persoanelor condamnate din bazele lor de date naționale create pentru prevenirea, depistarea și investigarea infracțiunilor. Respectivele 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; (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.			**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 bănuiți, învinuiți, inculpați și condamnați, extrase din bazele de date naționale. (2) Seturile de date puse la dispoziție prin intermediul 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		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **Articolul 21.** Căutarea automatizată în Registrul

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.			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, bănuiților, 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		Prevedere UE netranspusă	Prevederea urmează să se regăsească în reglementările interne privind evidența 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.			
Articolul 28. Norme privind solicitările și răspunsurile referitoare la evidențele 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.		Prevedere UE netranspusă	Prevederea urmează să se regăsească în reglementările interne privind evidența poliției
(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: (a) căutării persoanelor dispărute în contextul anchetelor penale sau din motive umanitare; (b) identificării de rămășițe umane.		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **Articolul 22.** Căutarea persoanelor dispărute fără veste, identificarea cadavrelor sau a părților acestuia (1) Autoritatea competentă de aplicare a legii este împuternicită 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		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **Articolul 22.** Căutarea persoanelor dispărute fără veste,

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).			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 Fiecare stat membru desemnează unul sau mai multe puncte de contact naționale în sensul articolelor 6, 11, 16, 20 și 26.		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 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		Prevedere UE neaplicabilă	Prevederile acestui articol se referă la competențele executive

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).			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	***Proiectul de lege privind cooperarea polițienească internațională*** **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 cazurile în care schimbul automatizat de date nu este disponibil.		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **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; 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	***Proiectul de lege privind cooperarea polițienească internațională***

			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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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 (bănuit, 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. Respectivele 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. Respectivele justificări 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 aflate în curs, acestea se șterg odată ce nu mai sunt necesare pentru procedurile de monitorizare.		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **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 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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		Compatibil	***Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale***

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.			***de Contact în scopul schimbului de date și informații*** **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.
(2) Orice schimb automatizat de date în conformitate cu prezentul regulament utilizează standardul UMF, în măsura în care este posibil.		Compatibil	***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** **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.
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.		Compatibil	***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 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.
(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; (c) o infrastructură de comunicații securizată între infrastructura centrală și portalul european de căutare, instituit prin articolul 6 din Regulamentul (UE) 2019/817		Compatibil	***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 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

și articolul 6 din Regulamentul (UE) 2019/818, în sensul articolului 39.			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.		Compatibil	***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 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.
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		Compatibil	***Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale***

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.			***de 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 bănuit 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.		Compatibil	***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 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.
(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.		Compatibil	***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 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.
(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.		Compatibil	***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 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.
(5) Routerul returnează utilizatorului routerului lista datelor biometrice între care s-a stabilit o concordanță și clasificarea acestora.		Compatibil	***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 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.
(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. 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 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 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*** 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.		Compatibil	***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 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.
Articolul 39. Interoperabilitatea dintre router și registrul comun de date de identitate în scopul accesului autorităților de aplicare a legii		Compatibil	***Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale***

(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.			***de 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 bănuit 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.		Compatibil	***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 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.
Interogările simultane în bazele de date ale statelor membre și în datele Europol și în		Compatibil	***Proiectul Hotărârii de Guvern cu privire la instituirea și***

registrul comun de date de identitate sunt lansate numai atunci când există motive 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.			***funcționarea Punctului Unic de Contact și a Punctelor Naționale de 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 bănuit 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	***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.
(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		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională***

prelucrării datelor, precum și pentru asigurarea securității și integrității datelor. Respectivele 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.			**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. (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	***Proiectul de lege privind cooperarea polițienească internațională*** **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 Europol în mod automatizat. Statul membru vizat ia măsuri corespunzătoare fără întârziere pentru a soluționa imposibilitatea tehnică de a utiliza routerul.		Compatibil	***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 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 ***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***, 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.		Compatibil	***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 46. Pentru căutarea de date în registrele naționale ale evidențelor poliției, PUC utilizează sistemul EPRIS ca infrastructură tehnică de interconectare.
(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.		Compatibil	***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 47. S**istemul 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; 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.		Compatibil	***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 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.
(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.		Compatibil	***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 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.
(3) Datele menționate la alineatul (1) literele (a) și (b) și la alineatul (2) litera (a), trebuie să fie pseudonimizate.		Compatibil	***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 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 algoritmii 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.		Compatibil	***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 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.
(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.		Compatibil	***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 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.		Compatibil	***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 69.** Lista concordanțelor, precizând calitatea acestora și statul deținător al datelor, este returnată către PUC de către sistemul EPRIS în mod automatizat.
(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.		Compatibil	***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 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.

(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. 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 alineat vizează competențele executive ale Comisiei Europene și mecanismele de comitologie (procedura de examinare conform Regulamentului 182/2011) pentru stabilirea detaliilor tehnice ale 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	***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 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	***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.
(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.		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **Articolul 43.** Înregistrarea operațiunilor de acces și schimb de date

Respectivele 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.			(3) Înregistrările sunt utilizate pentru elaborarea de date statistice, pentru verificarea 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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		Prevedere UE neaplicabilă	Prevederile acestui alineat sunt incompatibile sub aspectul reglementării naționale, deoarece impun obligații de notificare automatizată și sarcini de

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.			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.		Compatibil	***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.
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		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

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 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.			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 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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;		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **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;

(i) infracțiunea pentru care au fost obținute datele biometrice; (j) numărul cauzei penale; (k) autoritatea competentă responsabilă de cauza penală.			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	***Proiectul de lege privind cooperarea polițienească internațională*** **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		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională***

face obiectul unei decizii luate de un factor uman.			**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.		Compatibil	***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 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.
(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		Compatibil	***Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de Contact și a Punctelor Naționale***

stocate de Europol, acțiunea ulterioară are loc în conformitate cu Regulamentul (UE) 2016/794.			***de Contact în scopul schimbului de date și informații*** **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.
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.		Compatibil	***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** **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.
(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 vehiculelor drept criteriu de căutare se efectuează utilizând Eucaris.		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.
(4) Interogările efectuate de Europol utilizând date biografice ale suspecților 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		Prevedere UE neaplicabilă	Prevederea nu este aplicabilă pentru transpunere în legislația Republicii Moldova, întrucât

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.			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; (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		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.

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 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.		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională***

scopurile menționate la alineatul (2) sau o asemenea prelucrare este autorizată în conformitate cu alineatul (1).			**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 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.		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **Articolul 46.** Protecția și scopul prelucrărilor datelor cu caracter personal (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 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.		Compatibil	***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 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; **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.		Compatibil	***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** **Punctul 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;
(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 de supraveghere sau a Autorității Europene pentru Protecția Datelor, după caz.		Compatibil	***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 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. **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.		Compatibil	***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;
În cazul în care există motive să se creadă că ștergerea datelor ar aduce atingere 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.		Compatibil	***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 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 creează 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.		Compatibil	***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 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.
(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 EPRIS, precum și a infrastructurii de comunicații aferente acestora.		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 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		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.

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; (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 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.		Compatibil	***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 5.** Prezentului Regulament, i se aplică noțiunile din Legea nr. XXX/2026 privind cooperarea polițienească internațională, precum și noțiunile utilizate cu următoarele semnificații: 5.6. *incident semnificativ de securitate cibernetică* – orice eveniment care are sau poate avea un impact major asupra funcționării infrastructurii Routerului 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.		Compatibil	***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 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.
(3) În cazul unui incident de securitate privind EPRIS, statele membre vizate și Europol cooperează între ele pentru a asigura un răspuns rapid, eficace și corespunzător.		Compatibil	***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 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.
(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 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		Compatibil	***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 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.

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.		Compatibil	***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 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.
(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.		Compatibil	***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 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.
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,		Parțial compatibilă	***Proiectul de lege privind cooperarea polițienească internațională*** **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.

cu Autoritatea Europeană pentru Protecția Datelor.			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 frecventă 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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 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.		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **Articolul 49.** Răspunderea (2) În cazul în care autoritatea competentă de aplicare a legii nu își îndeplinește obligațiile stabilite 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		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.

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.			
(2) eu-LISA și Europol pun la dispoziția Autorității Europene pentru Protecția Datelor 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.		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.
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.		Compatibil	***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 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.
(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.		Compatibil	***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 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.
(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		Compatibilă	***Proiectul de lege privind cooperarea polițienească internațională*** **Articolul 50.** Transferul de date cu caracter personal către țări terțe și organizații internaționale

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.			(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.
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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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,		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **Articolul 51.** Responsabilitatea și instruirea (2) Autoritățile competente asigură, după caz, personalului

pentru a îndeplini sarcinile prevăzute în prezentul regulament.			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;		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **Articolul 51.** Responsabilitatea și instruirea (5) Autoritățile competente desemnate potrivit prezentei legi, asigură:

(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; (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);			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 conectarea acesteia 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

(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.			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 EPRIIS 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 EPRIIS 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 EPRIIS de către Europol și adaptarea infrastructurii acesteia.
(4) Fără a aduce atingere căutărilor efectuate de Europol în temeiul articolului 49, Europol nu are acces la niciuna dintre datele cu caracter personal prelucrate prin intermediul EPRIS.		Prevedere UE neaplicabilă	Reglementează gestiunea tehnică a sistemului EPRIIS de către 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		Prevedere UE neaplicabilă	Reglementează gestiunea tehnică a sistemului EPRIIS de către Europol și adaptarea infrastructurii acesteia.

ceea ce privește timpul de răspuns pentru transmiterea de solicitări către bazele de date naționale în conformitate cu specificațiile tehnice.			
(6) Europol asigură formarea pentru utilizarea tehnică a EPRIS.		Prevedere UE neaplicabilă	Reglementează gestiunea tehnică a sistemului EPRIIS 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 EPRIIS de către Europol și adaptarea infrastructurii acesteia.
Articolul 66. Responsabilitățile eu-LISA în etapa de concepere și dezvoltare a routerului (1) eu-LISA se asigură că infrastructura centrală a routerului este exploatată în conformitate cu 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.
(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 acesteia 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 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.		Prevedere UE neaplicabilă	Stabilesc obligațiile eu-Lisa privind dezvoltarea și gestionarea 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		Prevedere UE neaplicabilă	Stabilesc obligațiile eu-Lisa privind dezvoltarea și gestionarea tehnică a Routerului central, fiind norme interne ale UE pentru agenția sa.

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.			
Articolul 67. Responsabilitățile eu-LISA după începerea funcționării routerului (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		Prevedere UE neaplicabilă	Prevederea stabilește responsabilitățile agenției Uniunii Europene eu-LISA în ceea ce privește funcționarea infrastructurii centrale a sistemului Prüm II (router).

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.			
(2) Fără a aduce atingere articolului 17 din Statutul funcționarilor Uniunii Europene prevăzut în Regulamentul (CEE, Euratom, 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.		Prevedere UE neaplicabilă	Prevederea stabilește responsabilitățile agenției Uniunii Europene eu-LISA în ceea ce 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		Compatibil	***Proiectul Hotărârii de Guvern cu privire la instituirea și funcționarea Punctului Unic de***

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 concordanțe cu baza de date a fiecărui stat membru pentru fiecare categorie de date; (d) numărul de concordanțe cu datele Europol pentru fiecare categorie de date; (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.			***Contact și a Punctelor Naționale de Contact în scopul schimbului de date și informații*** **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; 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.		Compatibil	***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 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; 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: (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.		Compatibil	***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 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; 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		Prevedere UE neaplicabilă	Prevederea reglementează repartizarea costurilor în bugetul

(1) Costurile aferente instituirii și funcționării routerului și a EPRIS sunt suportate din bugetul general al Uniunii.			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 faciale și a registrelor naționale ale evidențelor poliției pentru prevenirea, depistarea și investigarea infracțiunilor sunt suportate din bugetul general al Uniunii.		Prevedere UE neaplicabilă	Prevederea reglementează repartizarea costurilor în bugetul UE pentru integrarea infrastructurii naționale existente și conexiunile acesteia 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	***Proiectul de lege privind cooperarea polițienească internațională*** **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. Respectivele autorități pot utiliza routerul sau pot avea acces la acesta.		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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 căutările automatizate cărora li se aplică articolele 10 și 11.		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **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		Compatibil	***Proiectul de lege privind cooperarea polițienească internațională*** **Articolul 53.** Notificări

la condițiile pentru căutările automatizate cărora li se aplică articolele 19 și 20.			(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	***Proiectul de lege privind cooperarea polițienească internațională*** **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	***Proiectul de lege privind cooperarea polițienească internațională*** **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 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.		Prevedere UE neaplicabilă	Prevederea stabilește o competență exclusivă a Comisiei de a fixa data de utilizare pentru statele membre și Europol și 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: (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.		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 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;		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.

(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.			
(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 (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.		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 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		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

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.			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 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.		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.
(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. Respectivele rapoarte conțin informații detaliate cu privire 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.		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.

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.			
(3) Până la 26 aprilie 2025și, ulterior, în fiecare an în cursul etapei de dezvoltare a EPRIS, Europol prezintă Parlamentului European și Consiliului un raport privind stadiul dezvoltării EPRIS. Respectivele rapoarte conțin informații detaliate cu privire 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.		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.
(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 privind funcționarea tehnică a EPRIS, inclusiv în ceea ce privește securitatea 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.
(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;		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.

(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.			
(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). Respectivele 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). Respectivele 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 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. Respectivele 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.

AGENȚIA DE GUVERNARE ELECTRONICĂ

E-GOVERNANCE AGENCY

Republica Moldova, MD-2012, mun. Chișinău, bd. Ștefan cel Mare și Sfânt 134
Telefon: +373 22 820 026, email: office@egov.md, site-ul web: http://www.egov.md

Nr. 3007 – 135 din 28.05.2026
La nr. RRSI/_38/1826 din 06.05.2026

Ministerul Afacerilor Interne

Instituția publică „Agenția de Guvernare Electronică" a examinat ***proiectul de hotărâre cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale" și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale,*** prezentat pentru coordonare prealabilă, și, în limitele competențelor instituției, comunică următoarele obiecții și propuneri.

Comentariu și obiecție de ordin general:

1. Conform Notei de fundamentare, la descrierea temeiului legal de la pct. 2 se menționează *„Temeiul legal de inițiere al acestui proiect de hotărâre, derivă din acțiunea nr.26 din Capitolul 24 Justiție, libertate și securitate, Cluster 1, Anexa A, din Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025 - 2029, aprobat prin Hotărârea Guvernului nr. 306/2025, care prevede stabilirea unei baze de date privind imaginile faciale ale infractorilor și înregistrarea imaginilor suspecților și persoanelor condamnate (opțional victimele), ca o condiție prealabilă pentru schimburile automate de imagini faciale Prüm, în conformitate cu Deciziile 2008/615/JAI ale Consiliului, modificate prin Regulamentul Prüm II 2024/982."* Totodată, **art. 19** din Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024 privind căutarea și schimbul automatizat de date în scopul cooperării polițienești, 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 prevede că *„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"*.

Subsecvent, denumirea și textul proiectului se vor revizui pentru a reda întocmai temeiul legal, pentru a reda categoriile de persoane pentru care vor fi preluate imaginile faciale, excluzând astfel interpretarea eronată a obiectului de reglementare.

La proiectul Conceptului:

2. La **pct. 6,** cuvântul „automatizat" urmează a fi exclus, iar norma urmează a fi expusă în corelare cu noțiunea de „sistem informațional" reglementată de art. 3 din Legea nr. 467/2003 cu privire la informatizare și resursele informaționale de stat, definită ca „totalitate de resurse (totalitate de informaţii documentate în sistemele informaţionale automatizate, organizată în conformitate cu cerinţele stabilite şi cu legislaţia în vigoare) şi tehnologii informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie".

3. La **pct. 7**, clasificarea resursei informaționale urmează a fi corelată cu clasificarea reglementată de art. 11 alin.(3) din Legea nr. 467/2003.

4. Capitolul III:

4.1 La **subpct. 19.8** recomandăm înlocuirea referinței la *„Legea nr. 133/2011 privind protecția datelor cu caracter personal"* cu referința la *„Legea nr. 195/2024 privind protecția datelor cu caracter personal"*, având în vedere că Legea nr. 133/2011 urmează a fi abrogată odată cu intrarea în vigoare a Legii nr. 195/2024. Această obiecție este aplicabilă și pentru orice altă trimitere la „Legea nr. 133/2011" regăsită în textul proiectului Conceptului și al Regulamentului (inclusiv pct. 4.4.1 din Nota de fundamentare), care urmează a fi corelate corespunzător.

4.2 Pct. 19 urmează a fi completat cu un subpunct nou care să facă referință la „*Hotărârea Guvernului nr. 677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design".* În acest sens, menționăm că în conformitate cu prevederile pct. 10 din Hotărârea citată mai sus *„Se recomandă autorităților publice, altele decât cele menționate la pct. 7, aplicarea modelului unitar de design la crearea sau dezvoltarea altor resurse și sisteme informaționale de stat care nu sunt destinate prestării serviciilor publice electronice sau la crearea și dezvoltarea noilor site-uri web oficiale, precum și coordonarea designului elaborat cu Instituția publică „Agenția de Guvernare Electronică"."* Detalii despre structura modelului unitar și pașii necesari pentru coordonare și implementare pot fi găsite la adresa https://mud.egov.md.

5. La **pct. 29**, cuvintele *„prin intermediul platformei de interoperabilitate și al altor servicii guvernamentale partajate aplicabile"* se vor substitui cu cuvintele „*prin intermediul platformei de interoperabilitate (MConnect)",* în conformitate cu prevederile Legii nr. 142/2018 cu privire la schimbul de date și interoperabilitate.

6. Cu referire la lista subiecților SI RIF prevăzută la **pct. 36,** atragem atenția asupra faptului că, potrivit art. 23 alin. (3) din Legea nr. 467/2003, Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică" (STISC) *„administrează infrastructura tehnologiilor informaționale ale autorităților și instituțiilor publice, exercită atribuțiile administratorului tehnic și asigură mentenanța sistemelor informaționale de stat, asigură securitatea cibernetică a acestora, precum și exercită și alte atribuții în conformitate cu statutul acesteia aprobat de către Guvern"*. În acest sens, lista subiecților raporturilor juridice aferente SI RIF urmează a fi structurată după modelul art. 7 din Legea nr. 467/2003 prin includerea „administratorului tehnic". Totodată, prin prisma art. 23 alin. (3) din Legea nr. 467/2003 și prevederilor Hotărârii nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, aspectele ce țin de administrarea tehnică și găzduire a resurselor și sistemelor informaționale urmează a fi coordonate cu STISC.

7. La **Capitolul VII Secțiunea 1**, în conformitate cu prevederile **pct.2.2.7** din Structura concepției sistemului din Anexa nr. 3 la Reglementarea tehnică „Procesele ciclului de viață al software-ului" RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78/2006, obiectele informaționale care sunt împrumutate din alte sisteme urmează să fie reglementate expres în textul proiectului. Totodată, la descrierea identificatorilor obiectelor informaționale de la secțiunea menționată urmează a fi respectate prevederile art. 19 alin. (8) din Legea nr. 71/2007 cu privire la registre care stabilește că *„Înregistrarea repetată a obiectului registrului, care a fost înregistrat într-un alt registru de stat, sau acumularea repetată a datelor despre obiect în acelaşi registru se interzice"*. În acest sens, pentru obiectele informaționale împrumutate urmează a fi prevăzut identificatorul descris în sistemul/resursa informațională din care este împrumutat, în special IDNP pentru persoanele fizice și IDNO pentru unitățile de drept, iar atributele precum „datele de identificare ale persoanei" și „identificatorul persoanei din sistemul-sursă interoperabil" urmează a fi clarificate și ajustate corespunzător.

8. La **pct. 71**, urmează a fi inclusă componenta MConnect Events ca element distinct al platformei guvernamentale de interoperabilitate. Având în vedere că SI RIF generează evenimente cu efecte operaționale asupra fluxurilor de prelucrare a datelor (confirmarea/infirmarea concordanței, modificarea statutului obiectelor informaționale, suspendarea sau retragerea datelor din setul destinat schimbului transfrontalier etc.), se propune expunerea punctului cu următorul cuprins:

„71. Pentru înregistrare și schimb de date, în cadrul SI RIF, acesta interacționează, prin intermediul platformei guvernamentale de interoperabilitate (MConnect), inclusiv cu utilizarea MConnect Events prin interfețe de programare a

aplicațiilor (API), pentru expunerea evenimentelor în timp real, în conformitate cu ghidul tehnic publicat de AGE, cu următoarele sisteme informaționale partajate: ...";

Subpunctele aferente fiecărui sistem informațional partajat (MPass, MSign, MLog, MNotify) urmează a fi păstrate, iar subpunctul privind MConnect va fi exclus din enumerare, norma respectivă fiind preluată în corpul pct. 71.

Redacția propusă urmează a fi preluată și pentru redactarea corespunzătoare a Capitolului VIII Secțiunea a 2-a din proiectul Regulamentului.

9. În conformitate cu pct. 4 subpct. 1) din Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog), în pct. 114 cuvintele „după caz" se vor substitui cu cuvintele „precum și".

La proiectul Regulamentului:

10. Pct. 4 urmează a fi ajustat în conformitate cu obiecția nr. 3 din prezentul aviz.

11. La **pct. 6** sintagma „cadrul normativ aplicabil" urmează a fi ajustată în conformitate cu prevederile art. 54 din Legea nr. 100/2017 cu privire la actele normative, pentru a evita interpretarea eronată.

12. Capitolul II se va exclude, acesta conținând norme care dublează prevederile proiectului de Concept și sunt improprii unui Regulament.

13. Lista subiecților reglementată în **Capitolul III** și care enumeră exhaustiv „registratorii", „furnizorii" și „destinatarii" urmează a fi corelată cu lista subiecților de la **Capitolul V din proiectul Conceptului**.

Director adjunct **Andrei PRISACAR**

Ex.: Vlad Luca,
e-mail: vlad.luca@egov.md,
tel.: 062061565

SINTEZA
la proiectul de hotărâre cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale

Participantul la avizare, consultare publică, expertizare	Nr. crt.	Conținutul obiecției, propunerii, recomandării, concluziei	Argumentarea autorului proiectului
Coordonare prealabilă			
Instituția publică „Agenția de Guvernare Electronică” (aviz prealabil nr. 3007-135 din 28 mai 2026)	**1.**	**1.** Conform Notei de fundamentare, la descrierea temeiului legal de la pct. 2 se menționează *„Temeiul legal de inițiere al acestui proiect de hotărâre, derivă din acțiunea nr.26 din Capitolul 24 Justiție, libertate și securitate, Cluster 1, Anexa A, din Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025 - 2029, aprobat prin Hotărârea Guvernului nr. 306/2025, care prevede stabilirea unei baze de date privind imaginile faciale ale infractorilor și înregistrarea imaginilor suspecților și persoanelor condamnate (opțional victimele), ca o condiție prealabilă pentru schimburile automate de imagini faciale Prüm, în conformitate cu Deciziile 2008/615/JAI ale Consiliului, modificate prin Regulamentul Prüm II 2024/982.”* Totodată, **art. 19** din Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024 privind căutarea și schimbul automatizat de date în scopul cooperării polițienești, 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 prevede că *„Statele membre asigură disponibilitatea datelor de referință privind imaginile faciale ale suspecților, ale persoanelor condamnate și, în cazul în care*	**Se acceptă parțial.** Textul proiectului a fost revizuit în vederea delimitării clare dintre componenta națională a Registrului imaginilor faciale și setul de date de referință destinat schimbului automatizat transfrontalier. Categoriile de persoane eligibile pentru includerea în setul de date de referință destinat schimbului automatizat transfrontalier au fost corelate cu art. 19 din Regulamentul (UE) 2024/982. Totodată, se menține denumirea proiectului, întrucât acesta reglementează sistemul informațional național „Registrul imaginilor faciale”, iar nu exclusiv componenta de schimb automatizat transfrontalier Prüm II. Prin urmare, au fost efectuate modificările necesare la pct. 10.3, 10.4 din Concept, iar conform recomandărilor capitolul II a fost exclus din Regulament și completată Nota de fundamentare

		dreptul intern permite acest lucru, ale victimelor, din bazele lor de date naționale create pentru prevenirea, depistarea și investigarea infracțiunilor”. Subsecvent, denumirea și textul proiectului se vor revizui pentru a reda întocmai temeiul legal, pentru a reda categoriile de persoane pentru care vor fi preluate imaginile faciale, excluzând astfel interpretarea eronată a obiectului de reglementare.	
	2.	**La proiectul Conceptului:** **2.** La **pct. 6,** cuvântul „automatizat” urmează a fi exclus, iar norma urmează a fi expusă în corelare cu noțiunea de „sistem informațional” reglementată de art. 3 din Legea nr. 467/2003 cu privire la informatizare și resursele informaționale de stat, definită ca „totalitate de resurse (totalitate de informaţii documentate în sistemele informaţionale automatizate, organizată în conformitate cu cerinţele stabilite şi cu legislaţia în vigoare) şi tehnologii informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie”.	**Se acceptă.**
	3.	**3.** La **pct. 7**, clasificarea resursei informaționale urmează a fi corelată cu clasificarea reglementată de art. 11 alin.(3) din Legea nr. 467/2003.	**Se acceptă.**
	4.	**4. Capitolul III:** **4.1** La **subpct. 19.8** recomandăm înlocuirea referinței la *„Legea nr. 133/2011 privind protecția datelor cu caracter personal”* cu referința la *„Legea nr. 195/2024 privind protecția datelor cu caracter personal”*, având în vedere că Legea nr. 133/2011 urmează a fi abrogată odată cu intrarea în vigoare a Legii nr. 195/2024. Această obiecție este aplicabilă și pentru orice altă trimitere la „Legea nr. 133/2011” regăsită în textul proiectului Conceptului și al Regulamentului (inclusiv pct. 4.4.1 din Nota de fundamentare), care urmează a fi corelate corespunzător.	**Se acceptă.**

	5.	**4.2 Pct. 19** urmează a fi completat cu un subpunct nou care să facă referință la *„Hotărârea Guvernului nr. 677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design”*. În acest sens, menționăm că în conformitate cu prevederile pct. 10 din Hotărârea citată mai sus *„Se recomandă autorităților publice, altele decât cele menționate la pct. 7, aplicarea modelului unitar de design la crearea sau dezvoltarea altor resurse și sisteme informaționale de stat care nu sunt destinate prestării serviciilor publice electronice sau la crearea și dezvoltarea noilor site-uri web oficiale, precum și coordonarea designului elaborat cu Instituția publică „Agenția de Guvernare Electronică”.”* Detalii despre structura modelului unitar și pașii necesari pentru coordonare și implementare pot fi găsite la adresa https://mud.egov.md.	**Se acceptă.**
	6.	**5.** La pct. 29, cuvintele „prin intermediul platformei de interoperabilitate și al altor servicii guvernamentale partajate aplicabile” se vor substitui cu cuvintele „prin intermediul platformei de interoperabilitate (MConnect)”, în conformitate cu prevederile Legii nr. 142/2018 cu privire la schimbul de date și interoperabilitate.	**Se acceptă.**
	7.	**6.** Cu referire la lista subiecților SI RIF prevăzută la **pct. 36,** atragem atenția asupra faptului că, potrivit art. 23 alin. (3) din Legea nr. 467/2003, Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică” (STISC) *„administrează infrastructura tehnologiilor informaționale ale autorităților și instituțiilor publice, exercită atribuțiile administratorului tehnic și asigură mentenanța sistemelor informaționale de stat, asigură securitatea cibernetică a acestora, precum și exercită și alte atribuții în conformitate cu statutul acesteia aprobat de către Guvern”*. În acest sens, lista subiecților raporturilor	**Se acceptă.** Lista subiecților SI RIF a fost completată cu categoria „administratorul tehnic al sistemului”, în vederea corelării cu art. 7 din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat. Totodată, în proiect au fost delimitate atribuțiile deținătorului SI RIF, exercitate de Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne, de atribuțiile administratorului

		juridice aferente SI RIF urmează a fi structurată după modelul art. 7 din Legea nr. 467/2003 prin includerea „administratorului tehnic”. Totodată, prin prisma art. 23 alin. (3) din Legea nr. 467/2003 și prevederilor Hotărârii nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, aspectele ce țin de administrarea tehnică și găzduire a resurselor și sistemelor informaționale urmează a fi coordonate cu STISC.	tehnic, exercitate de Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, în limitele competențelor stabilite de art. 23 alin. (3) din Legea nr. 467/2003 și de Hotărârea Guvernului nr. 414/2018. Aspectele privind găzduirea și administrarea tehnică a infrastructurii vor fi coordonate cu STISC, fără a afecta atribuțiile MAI și ale STI al MAI privind guvernanța, dezvoltarea, administrarea, securitatea operațională și utilizarea SI RIF în scopurile prevăzute de lege.
	8.	**7.** La **Capitolul VII Secțiunea 1**, în conformitate cu prevederile **pct.2.2.7** din Structura concepției sistemului din Anexa nr. 3 la Reglementarea tehnică „Procesele ciclului de viață al software-ului” RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78/2006, obiectele informaționale care sunt împrumutate din alte sisteme urmează să fie reglementate expres în textul proiectului. Totodată, la descrierea identificatorilor obiectelor informaționale de la secțiunea menționată urmează a fi respectate prevederile art. 19 alin. (8) din Legea nr. 71/2007 cu privire la registre care stabilește că „*Înregistrarea repetată a obiectului registrului, care a fost înregistrat într-un alt registru de stat, sau acumularea repetată a datelor despre obiect în acelaşi registru se interzice”*. În acest sens, pentru obiectele informaționale împrumutate urmează a fi prevăzut identificatorul descris în sistemul/resursa informațională din care este împrumutat, în special IDNP pentru persoanele fizice și IDNO pentru unitățile de drept, iar atributele precum „datele de identificare ale persoanei” și „identificatorul persoanei din sistemul-sursă interoperabil” urmează a fi clarificate și ajustate corespunzător.	**Se acceptă.** Operate modificări la pct. 51–60 din Concept, iar ulterior reflectate corespunzător în Regulament, în partea privind categoriile de date, interoperabilitatea și regulile de validare.

	9.	La **pct. 71**, urmează a fi inclusă componenta MConnect Events ca element distinct al platformei guvernamentale de interoperabilitate. Având în vedere că SI RIF generează evenimente cu efecte operaționale asupra fluxurilor de prelucrare a datelor (confirmarea/infirmarea concordanței, modificarea statutului obiectelor informaționale, suspendarea sau retragerea datelor din setul destinat schimbului transfrontalier etc.), se propune expunerea punctului cu următorul cuprins: *„71. Pentru înregistrare și schimb de date, în cadrul SI RIF, acesta interacționează, prin intermediul platformei guvernamentale de interoperabilitate (MConnect), inclusiv cu utilizarea MConnect Events prin interfețe de programare a* *aplicațiilor (API), pentru expunerea evenimentelor în timp real, în conformitate cu ghidul tehnic publicat de AGE, cu următoarele sisteme informaționale partajate: ...”;* Subpunctele aferente fiecărui sistem informațional partajat (MPass, MSign, MLog, MNotify) urmează a fi păstrate, iar subpunctul privind MConnect va fi exclus din enumerare, norma respectivă fiind preluată în corpul pct. 71. Redacția propusă urmează a fi preluată și pentru redactarea corespunzătoare a Capitolului VIII Secțiunea a 2-a din proiectul Regulamentului.	**Se acceptă.** Pct. 71 (în redacția finală pct. 75) din Concept a fost expus în redacție nouă. Pentru Capitolul VII, Secțiunea a 2-a din Regulament, a fost reformulat pct. 152 - 154.
	10.	În conformitate cu pct. 4 subpct. 1) din Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog), în pct. 114 cuvintele „după caz” se vor substitui cu cuvintele „precum și”.	**Se acceptă.** În redacția finală pct. 119
	11.	Pct. 4 urmează a fi ajustat în conformitate cu obiecția nr. 3 din prezentul aviz.	**Se acceptă.**
	12.	La pct. 6 sintagma „cadrul normativ aplicabil” urmează a fi ajustată în conformitate cu prevederile art. 54 din Legea nr. 100/2017 cu privire la actele normative, pentru a evita interpretarea eronată.	**Se acceptă.**

	13.	Capitolul II se va exclude, acesta conținând norme care dublează prevederile proiectului de Concept și sunt improprii unui Regulament.	**Se acceptă.**
	14.	Lista subiecților reglementată în Capitolul III și care enumeră exhaustiv „registratorii”, „furnizorii” și „destinatarii” urmează a fi corelată cu lista subiecților de la Capitolul V din proiectul Conceptului.	**Se acceptă.** În redacția finală Capitolul II

Secretar general al ministerului **Valentin CIOCLEA**

Ministerul Afacerilor Interne
al Republicii Moldova

Nr. 38/2341 din 09 iunie 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 aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale.
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 *(PNA, PND, PNR, alte documente de planificare sectoriale)*	Inițierea acestui proiect de act normativ rezidă din acțiunea operațională nr. 57 din Clusterul 1. Valori fundamentale, Capitolul 24 „Justiție, libertate și Securitate” al Programului național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 20252029, aprobat prin Hotărârea Guvernului nr. 306/2025.
5.	Lista autorităților și instituțiilor a căror avizare este necesară	*Avizare:* 1. Ministerul Justiției (inclusiv Administrația Națională a Penitenciarelor și Inspectoratul Național de Probațiune) 2. Ministerul Finanțelor (inclusiv Serviciul Vamal și Serviciul Fiscal de Stat); 3. Ministerul Dezvoltării Economice și Digitalizării; 4. Agenția de Guvernare Electronică;

		5. Centrul Național pentru Protecția Datelor cu Caracter Personal; 6. Agenția Servicii Publice; 7. Procuratura Generală; 8. Serviciul de Informații și Securitate; 9. Serviciul Tehnologia Informației și Securitate Cibernetică. *Expertizare:* 1. Ministerul Justiției; 2. Centrul Național Anticorupție; 3. Centrul de Armonizare a Legislației.
6.	Termenul-limită pentru depunerea avizelor/expertizelor	10 zile lucrătoare.
7.	Persoana responsabilă de promovarea proiectului	Vitalie Railean, șef al Secției politici în domeniul ordinii și securității publice a Direcției politici în domeniul ordinii și securității publice, combaterii criminalității a Ministerului Afacerilor Interne; telefon: 069688730, e-mail:vitalie.railean@mai.gov.md.
8.	Anexe	1. Proiectul actului normativ; 2. Nota de fundamentare; 3. Tabelul de concordanță; 4. Aviz prealabil AGE; 5. Sinteza obiecțiilor și propunerilor AGE.
9.	Data și ora depunerii cererii	
10.	Semnătura	**Valentin CIOCLEA,** **Secretar general al ministerului**