UE

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din 2026

Chișinău

Cu privire la aprobarea Conceptului Sistemului informațional „Registrul imaginilor faciale” și a Regulamentului privind modul 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, al 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, precum și al art. 17 alin. (2) și art. 19 alin. (8) din Legea nr. 209/2026 privind cooperarea polițienească internațională (Monitorul Oficial al Republicii Moldova, 2026, nr. 486-489, art. 505), Guvernul HOTĂRĂŞTE:

Prezenta hotărâre pune în aplicare parțial art. 19-24 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), CELEX: 32024R0982, publicat în Jurnalul Oficial al Uniunii Europene, seria L 2024/982 din 5 aprilie 2024.

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 modul de ținere a Registrului imaginilor faciale, conform anexei nr. 2.

3. Ministerul Afacerilor Interne va asigura condițiile juridice, financiare și organizatorice necesare pentru crearea, administrarea, mentenanța și dezvoltarea Sistemului informațional „Registrul imaginilor faciale”.

4. Crearea, dezvoltarea, administrarea, mentenanța și funcționarea Sistemului informațional „Registrul imaginilor faciale” se vor realiza din contul și în limitele mijloacelor financiare aprobate anual în bugetul Ministerului Afacerilor Interne, precum și din alte surse neinterzise de lege.

5. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Afacerilor Interne.

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

Prim-ministru **VASILE TOFAN**

Contrasemnează:

Ministrul dezvoltării
economice și digitalizării Claudiu-Iulius-Gavril Năsui

Ministrul afacerilor interne Daniella Misail-Nichitin

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

CONCEPTUL
Sistemului informațional „Registrul imaginilor faciale”

Capitolul I
INTRODUCERE

1. Prezentul Concept stabilește cadrul general pentru crearea, dezvoltarea și funcționarea Sistemului informațional „Registrul imaginilor faciale” (denumit 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 ale tratatelor internaționale.

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

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

5. Prezentul Concept definește scopul, obiectivele și principiile de funcționare ale SI RIF, structura generală a acestuia, categoriile de subiecți implicați, precum și cerințele generale de interoperabilitate și securitate și constituie temeiul conceptual pentru aprobarea Regulamentului privind modul de ținere a Registrului imaginilor faciale.

Capitolul II
DISPOZIȚII GENERALE

6. SI RIF este un sistem informațional distinct și specializat, constituit din resurse informaționale, tehnologii informaționale interdependente, metode și

personal, destinat formării, administrării, păstrării, prelucrării, furnizării și utilizării informațiilor privind imaginile faciale și a datelor de referință aferente acestora, inclusiv în vederea realizării schimbului automatizat transfrontalier de date de referință privind imaginile faciale, în condițiile prevăzute de actele normative, de cadrul normativ aplicabil cooperării polițienești internaționale și de tratatele internaționale.

7. Registrul imaginilor faciale (denumit în continuare *RIF*) 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, metadatele aferente, precum și informații privind rezultatele comparării automatizate.

8. În RIF 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 evidențiază ca atare.

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

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

10.1. componenta națională a RIF, care cuprinde totalitatea imaginilor faciale, a metadatelor aferente, a informațiilor asociate, a rezultatelor comparării automatizate și a altor date necesare pentru exercitarea atribuțiilor autorităților competente, în condițiile prevăzute de actele normative;

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

10.3. setul de date de referință privind imaginile faciale, destinat schimbului automatizat transfrontalier de date, se constituie, în condițiile legii privind cooperarea polițienească internațională și ale actelor normative adoptate în executarea acesteia, numai pentru categoriile de persoane care au calitatea de bănuit, învinuit, inculpat sau condamnat pentru săvârșirea infracțiunilor, precum și, în cazurile, condițiile și limitele prevăzute expres de cadrul normativ național în domeniul cooperării polițienești internaționale și de actele de punere în aplicare a acestuia, pentru victime, cu respectarea principiilor necesității, proporționalității, limitării scopului și protecției datelor cu caracter personal;

10.4. imaginile faciale aferente persoanelor dispărute fără veste, cadavrelor ori părților acestora pot fi gestionate în componenta națională a RIF, în condițiile prevăzute de actele normative, exclusiv pentru exercitarea 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 de date;

10.5. datele gestionate prin SI RIF se supun unor regimuri distincte de prelucrare, păstrare, utilizare și radiere, diferențiate cel puțin pentru următoarele categorii:

10.5.1. persoanele care au calitatea de bănuit, învinuit sau inculpat;

10.5.2. persoanele condamnate pentru săvârșirea unei infracțiuni;

10.5.3. victimele, în cazurile și limitele prevăzute expres de cadrul normativ național în domeniul cooperării polițienești internaționale, de tratatele internaționale la care Republica Moldova este parte și de actele de punere în aplicare a acestora;

10.5.4. persoanele dispărute fără veste;

10.5.5. cadavrele ori părțile acestora;

10.5.6. imaginile faciale neidentificate colectate în cadrul prevenirii, constatării sau investigării infracțiunilor, al căutării persoanelor dispărute ori al identificării cadavrelor sau a părților acestora.

11. Datele de referință privind imaginile faciale puse la dispoziție prin intermediul SI RIF nu conțin date suplimentare care să permită identificarea directă a persoanei. Datele de identificare ale persoanei și alte informații suplimentare pot fi extrase și furnizate numai după confirmarea concordanței și numai în condițiile prevăzute de actele normative.

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

12.1. *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 unui cadavru sau a unor părți ale acestuia;

12.2. *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 prevăzute de actele normative;

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

12.4. *imagine facială* – imagine digitală a feței unei persoane;

12.5. *imagine facială identificată* – imagine facială asociată unei persoane identificate;

12.6. *imagine facială neidentificată* – imagine facială colectată în cursul prevenirii, constatării sau investigării unei infracțiuni ori în cadrul căutării unei persoane dispărute sau al identificării unui cadavru ori a unor părți ale acestuia, care nu este asociată, la momentul introducerii, unei persoane identificate;

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

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

12.9. s*et de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier* – ansamblu distinct de date de referință extrase din SI RIF și puse la dispoziție pentru căutarea automatizată transfrontalieră, în condițiile prevăzute de actele normative;

12.10. *validarea concordanței* – verificarea de către personal calificat a rezultatului comparării automatizate, în condițiile prevăzute de actele normative.

13. Scopul SI RIF constă în asigurarea suportului informațional și funcțional necesar autorităților competente pentru prelucrarea imaginilor faciale, identificarea biometrică facială și validarea concordanțelor, precum și pentru constituirea și utilizarea, în condițiile prevăzute de actele normative, a setului de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier de date.

14. Obiectivele SI RIF sunt următoarele:

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

14.2. asigurarea comparării automatizate a imaginilor faciale și a generării 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 prevăzute de actele normative, a rezultatului tehnic preliminar al comparării automatizate și, după caz, a concordanțelor posibile identificate în urma acesteia;

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

14.5. asigurarea disponibilității setului de date de referință privind imaginile faciale în scopul schimbului automatizat transfrontalier de date cu autoritățile competente străine și, după caz, cu alte entități abilitate prin lege, exclusiv în condițiile prevăzute de cadrul normativ;

14.6. asigurarea interoperabilității cu sistemele și resursele informaționale relevante ale statului, fără substituirea funcțiilor 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, implementarea și utilizarea SI RIF se respectă următoarele principii:

15.1. principiul legalității, potrivit căruia crearea, administrarea și utilizarea SI RIF, precum și prelucrarea datelor din RIF se realizează numai în temeiul și în limitele cadrului normativ;

15.2. principiul necesității și proporționalității, potrivit căruia prelucrarea datelor se efectuează numai în măsura necesară pentru realizarea scopurilor determinate și legitime pentru care este instituit SI RIF;

15.3. principiul limitării scopului, potrivit căruia datele sunt colectate și prelucrate numai în scopuri determinate, explicite și legitime și nu sunt utilizate ulterior într-un mod incompatibil cu aceste scopuri;

15.4. principiul exactității și actualității datelor, potrivit căruia datele gestionate în RIF trebuie să fie exacte, relevante și actualizate, iar, după caz, să fie rectificate, completate, restricționate sau radiate în condițiile cadrului normativ;

15.5. principiul limitării stocării, potrivit căruia datele se păstrează într-o formă care permite identificarea persoanelor vizate numai pe perioada necesară realizării scopurilor pentru care sunt prelucrate, în conformitate cu termenele și criteriile stabilite de cadrul normativ;

15.6. principiul securității și confidențialității, potrivit căruia datele gestionate în RIF sunt protejate, prin măsuri tehnice și organizatorice adecvate, împotriva accesului neautorizat, divulgării, modificării, pierderii, distrugerii sau prelucrării neconforme;

15.7. principiul responsabilității și trasabilității, potrivit căruia operațiunile efectuate în SI RIF sunt atribuite utilizatorilor autorizați, documentate, jurnalizate și verificabile, pentru asigurarea controlului, auditului și răspunderii în condițiile legii.

16. Căutarea automatizată a datelor de referință privind imaginile faciale în cadrul componentei destinate schimbului automatizat transfrontalier se

efectuează exclusiv în cazuri individuale și în condițiile prevăzute de actele normative. Se interzice utilizarea datelor gestionate prin SI RIF pentru efectuarea unor interogări generale, exploratorii sau nedeterminate, precum și pentru crearea unor profiluri discriminatorii.

17. Modul de organizare și ținere a RIF, delimitarea componentei naționale a RIF de setul de date de referință destinat schimbului automatizat transfrontalier de date, categoriile de persoane ale căror date pot fi incluse în acest set, categoriile de date, temeiurile pentru introducerea, actualizarea, rectificarea, blocarea, radierea și arhivarea datelor, precum și condițiile de acces, comparare, validare, schimb automatizat, înregistrare în jurnalele de sistem și control se stabilesc prin Regulamentul privind modul de ținere a Registrului imaginilor faciale.

Capitolul III
CADRUL NORMATIV-JURIDIC AL SI RIF

18. Funcționarea SI RIF se realizează în temeiul Constituției Republicii Moldova, al tratatelor internaționale la care Republica Moldova este parte, precum și al cadrului normativ național în domeniul cooperării polițienești internaționale, al resurselor informaționale de stat, al registrelor, al schimbului de date și interoperabilității, al protecției datelor cu caracter personal, al securității cibernetice și al activității autorităților competente.

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

19.1. Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, semnată la Roma la 4 noiembrie 1950;

19.2. Convenția Consiliului Europei pentru protecția persoanelor față de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981;

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

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

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

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

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

19.8. 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;

19.9. Codul de executare nr. 443/2004;

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

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

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

19.13. Legea integrității nr. 82/2017;

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

19.15. Legea nr. 300/2017 cu privire la sistemul administrației penitenciare;

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

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

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

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

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

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

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

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

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

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

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

19.27. Hotărârea Guvernului nr. 716/2014 pentru aprobarea Regulamentului cu privire la Registrul persoanelor reținute, arestate şi condamnate;

19.28. 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;

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

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

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

19.32. 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;

19.33. 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);

19.34. 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;

19.35. 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”;

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

19.37. 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;

19.38. 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;

19.39. Ordinul ministrului dezvoltării informaționale nr. 78/2006 cu privire la aprobarea Reglementării tehnice „Procesele ciclului de viață al software-ului” RT 38370656-002:2006;

19.40. Standardul Republicii Moldova SM ISO/CEI 12207:2014 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al software-ului”;

19.41. Standardul Republicii Moldova SM ISO/CEI/IEEE 15288:2015 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al sistemului”;

19.42. Standardul Republicii Moldova SM ISO/CEI 27002:2017 „Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației”.

20. SI RIF se instituie în contextul alinierii cadrului normativ la cerințele privind căutarea și schimbul automatizat transfrontalier de date în scopul cooperării polițienești internaționale, în partea referitoare la imaginile faciale, în condițiile prevăzute de cadrul normativ național în domeniul cooperării polițienești internaționale, de tratatele internaționale la care Republica Moldova este parte și de actele de punere în aplicare a acestora.

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 normativ în domeniul protecției datelor cu caracter personal, al securității informației și al securității cibernetice.

Capitolul IV
SPAȚIUL FUNCȚIONAL AL SI RIF, PROCESELE ȘI FUNCȚIILE SI RIF

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

23.3. componenta de comparare biometrică facială;

23.4. componenta de suport pentru identificarea cazului sau a persoanei;

23.5. componenta de validare a concordanței;

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

23.7. componenta de interoperabilitate cu sistemele informaționale externe utilizate în cadrul cooperării polițienești internaționale;

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 stocare a datelor comparative privind imaginile faciale asigură constituirea, stocarea și gestionarea mostrelor comparative și a

metadatelor aferente acestora, inclusiv prin preluarea datelor din sistemele și resursele informaționale interoperabile.

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

27. Componenta de suport pentru identificarea cazului sau a persoanei asigură extragerea și constituirea datelor de bază și a informațiilor suplimentare necesare identificării persoanei și, după caz, individualizării cazului, pe 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 personalul calificat, a rezultatului comparării automatizate și, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe, confirmarea sau infirmarea concordanței, precum și înregistrarea rezultatului validării.

29. Componenta de interoperabilitate cu sistemele și resursele informaționale naționale relevante asigură schimbul de date prin intermediul platformei de interoperabilitate (MConnect), fără substituirea funcțiilor de evidență primară ale sistemelor și resurselor 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 a acestora, constituirea, extragerea, furnizarea, recepționarea și schimbul automatizat transfrontalier al setului de date de referință privind imaginile faciale, transmiterea și recepționarea solicitărilor și răspunsurilor căutării automatizate, 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, a rolurilor și a drepturilor de acces;
31.2. administrarea nomenclatoarelor și a metadatelor de sistem;
31.3. jurnalizarea operațiunilor efectuate în SI RIF;
31.4. monitorizarea utilizării sistemului;
31.5. aplicarea măsurilor tehnice și organizatorice de securitate;

31.6. asigurarea auditului și a trasabilității 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, după confirmarea concordanței și în condițiile prevăzute de actele normative, 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 datelor de referință privind imaginile faciale și furnizarea, după confirmarea concordanței, a datelor de bază și a informațiilor suplimentare, prin canale autorizate;

32.10. jurnalizarea, monitorizarea și auditul operațiunilor.

33. SI RIF asigură funcționalități care permit:

33.1. utilizarea, în vederea comparării automatizate, a imaginilor faciale care corespund cerințelor minime de calitate stabilite de cadrul normativ, de standardele europene și internaționale, precum și de documentația tehnică a SI RIF;

33.2. delimitarea funcțională a componentei naționale a RIF de setul de date de referință destinat schimbului automatizat transfrontalier de date;

33.3. limitarea schimbului automatizat transfrontalier la datele strict necesare;

33.4. utilizarea numerelor de referință;

33.5. păstrarea istoricului actualizărilor și a rezultatelor comparării;

33.6. utilizarea componentei destinate schimbului automatizat transfrontalier de date numai în cazuri individuale;

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

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

Capitolul V
STRUCTURA ORGANIZAȚIONALĂ A SI RIF, FUNCȚIILE DE BAZĂ ȘI SUBIECȚII ACESTUIA

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

36. Subiecții raporturilor juridice aferente ținerii RIF și utilizării SI RIF sunt următorii:

36.1. proprietarul SI RIF și al RIF;
36.2. posesorul SI RIF și al RIF;
36.3. deținătorul SI RIF;
36.4. administratorul tehnic al SI RIF;
36.5. utilizatorii SI RIF.

37. Proprietarul SI RIF și al RIF este statul, care își exercită dreptul de proprietate asupra sistemului și registrului, precum și drepturile și atribuțiile privind gestionarea și utilizarea acestora, în condițiile prevăzute de actele normative.

38. Posesor al SI RIF și al RIF este Ministerul Afacerilor Interne, care asigură guvernanța instituțională a sistemului, coordonarea dezvoltării și utilizării acestuia, coordonarea proceselor aferente ținerii registrului și cooperarea dintre autoritățile participante, precum și, în condițiile prevăzute de actele normative, 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 din subordinea Ministerului Afacerilor Interne, care asigură crearea, dezvoltarea, mentenanța aplicației, funcționarea tehnică a acesteia, 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.

40. Administratorul tehnic al SI RIF este Instituția publică Serviciul Tehnologia Informației și Securitate Cibernetică, care asigură administrarea tehnică și menținerea SI RIF în conformitate cu Regulamentul privind administrarea tehnică și menținerea resurselor și sistemelor informaționale de stat, aprobat prin 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.

41. Utilizatorii SI RIF sunt persoanele fizice desemnate de către registratori, de către furnizorii de date și de către destinatarii datelor, cărora li se acordă acces autorizat la SI RIF în baza rolurilor atribuite, în conformitate cu politicile de securitate și de control al accesului și în limitele competențelor legale, în vederea efectuării operațiunilor asupra datelor din RIF, exclusiv în scopuri prevăzute de actele normative, de prezentul Concept și de Regulamentul privind modul de ținere a Registrului imaginilor faciale.

42. Registratorii sunt persoane autorizate, desemnate în condițiile prevăzute de actele normative, care efectuează, prin intermediul SI RIF, operațiuni asupra datelor din Registrul imaginilor faciale, inclusiv introducerea, actualizarea, rectificarea, completarea, blocarea, radierea și arhivarea datelor, marcarea imaginilor faciale neidentificate, atribuirea și verificarea numerelor de referință, ținerea evidenței acestora, actualizarea metadatelor aferente, înregistrarea solicitărilor și răspunsurilor aferente căutării automatizate, consemnarea rezultatelor comparării automatizate și a confirmării sau infirmării concordanței, precum și actualizarea datelor relevante pentru componenta destinată schimbului automatizat transfrontalier de date, în limitele competențelor stabilite de lege și exclusiv în scopurile prevăzute de cadrul normativ.

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

43.1. subdiviziunile specializate ale Inspectoratului General al Poliției;

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

43.3. subdiviziunile specializate ale Inspectoratului General pentru Migrație;

43.4. subdiviziunile specializate ale Centrului Național Anticorupție, exclusiv în raport cu cauzele, materialele, procedurile sau activitățile aflate în competența acestuia;

43.5. 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.

44. Registratorii desemnați pentru componenta destinată schimbului automatizat transfrontalier de date efectuează operațiuni numai în cazuri individuale, cu utilizarea numerelor de referință, cu respectarea cerințelor privind validarea, jurnalizarea și trasabilitatea, precum și a procedurilor privind

transmiterea și recepționarea solicitărilor și răspunsurilor aferente căutării automatizate, în condițiile prevăzute de actele normative.

45. Furnizorii sunt autoritățile și entitățile care furnizează, în condițiile prevăzute de actele normative, date, imagini faciale, metadate sau alte informații necesare constituirii, completării și actualizării RIF, inclusiv prin mecanisme de interoperabilitate, precum și, după caz, constituirii și actualizării setului de date de referință destinat schimbului automatizat transfrontalier de date, asigurând legalitatea furnizării, exactitatea, actualitatea, relevanța și integritatea datelor, precum și, după caz, calitatea corespunzătoare a imaginilor faciale pentru compararea automatizată.

46. Furnizorii de date pentru SI RIF sunt:

46.1. subdiviziunile specializate ale Inspectoratului General al Poliției;

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

46.3. subdiviziunile specializate ale Inspectoratului General pentru Migrație;

46.4. Agenția Servicii Publice;

46.5. Serviciul de Informații și Securitate;

46.6. Administrația Națională a Penitenciarelor;

46.7. Inspectoratul Național de Probațiune;

46.8. Centrul Național Anticorupție;

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

47. Destinatarii sunt autoritățile și instituțiile publice, precum și alte entități care au dreptul legal de a accesa sau primi date din RIF, prin intermediul SI RIF sau prin alte canale autorizate, în vederea realizării atribuțiilor ce le revin. După caz, destinatarii pot extrage și furniza datele de bază și informațiile suplimentare aferente unei concordanțe confirmate, prin canalele, procedurile și punctele de contact stabilite de cadrul normativ aplicabil schimbului automatizat transfrontalier de date, cu respectarea cerințelor privind accesul autorizat și diferențiat, necesitatea funcțională, jurnalizarea și trasabilitatea operațiunilor, precum și a interdicției de utilizare a datelor pentru interogări generale sau exploratorii ori în alte scopuri decât cele prevăzute de actele normative.

48. Destinatari ai datelor din RIF sunt 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:

48.1. subdiviziunile specializate ale Inspectoratului General al Poliției;

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

48.3. subdiviziunile specializate ale Inspectoratului General pentru Migrație;

48.4. Agenția Servicii Publice, în limitele competențelor prevăzute de actele normative;

48.5. Serviciul de Informații și Securitate, în limitele competențelor prevăzute de actele normative;

48.6. Administrația Națională a Penitenciarelor, în limitele competențelor prevăzute de actele normative;

48.7. Inspectoratul Național de Probațiune, în limitele competențelor prevăzute de actele normative;

48.8. Procuratura Generală, în condițiile actelor normative și în limitele atribuțiilor privind conducerea și exercitarea urmăririi penale;

48.9. Centrul Național Anticorupție, în limitele competențelor prevăzute de lege și exclusiv în volumul necesar exercitării atribuțiilor legale;

48.10. autoritățile și entitățile externe, în condițiile prevăzute de cadrul normativ național în domeniul cooperării polițienești internaționale, de tratatele internaționale la care Republica Moldova este parte și de actele de punere în aplicare a acestora;

48.11. alte autorități publice competente, în condițiile prevăzute de actele normative.

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

Capitolul VI
DOCUMENTELE ȘI DATELE SI RIF

50. În cadrul SI RIF se utilizează următoarele categorii de documente:

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

50.2. documente de ieșire, generate în urma procesării datelor și funcționării sistemului;

50.3. documente tehnologice, generate și utilizate pentru administrarea tehnică, exploatarea, securizarea și auditarea sistemului.

51. Documentele de intrare ale SI RIF sunt următoarele:

51.1. imaginile faciale recepționate din surse autorizate, în condițiile prevăzute de actele normative;

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

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

51.4. imaginile faciale recepționate în cadrul schimbului de date cu autoritățile competente naționale sau străine, în condițiile prevăzute de actele normative;

51.5. documentele și datele referitoare la persoanele identificate, în cazurile prevăzute de actele normative;

51.6. documentele și datele aferente imaginilor faciale neidentificate;

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

51.8. documentele și datele privind sursa imaginii faciale, precum și data și locul prelevării, captării sau extragerii acesteia;

51.9. documentele și datele privind temeiul legal pentru introducerea imaginii faciale în registru;

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

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

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

51.13. documentele și datele recepționate prin intermediul mecanismului de interoperabilitate, din alte sisteme informaționale și resurse informaționale relevante ale statului;

51.14. formularele standardizate de evidență, completate potrivit indicatorilor și cerințelor prevăzute de prezentul Concept și de Regulamentul privind modul de ținere a Registrului imaginilor faciale.

52. Documentele de ieșire ale SI RIF sunt următoarele:

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

52.2. extrasele individuale din Registrul imaginilor faciale, eliberate autorităților competente, în condițiile prevăzute de actele normative;

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

52.4. datele de bază și informațiile suplimentare furnizate după confirmarea concordanței, în condițiile prevăzute de actele normative;

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

52.6. seturile de date, mesajele și extrasele transmise în cadrul cooperării polițienești internaționale, în condițiile prevăzute de cadrul normativ național în domeniul cooperării polițienești internaționale, de tratatele internaționale la care Republica Moldova este parte și de actele de punere în aplicare a acestora;

52.7. rapoartele analitice și statistice privind utilizarea sistemului, volumul datelor prelucrate, rezultatele comparărilor și alte informații agregate, în condițiile prevăzute de actele normative;

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

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

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

53.2. jurnalele operațiunilor de accesare și prelucrare a datelor;

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

53.4. înregistrările privind rezultatele comparării automatizate;

53.5. înregistrările privind confirmarea sau infirmarea concordanței;

53.6. jurnalele de acces și evidențele incidentelor de securitate, inclusiv alertele de monitorizare;

53.7. fișele de control, monitorizare și audit;

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

53.9. documentația tehnică aferentă SI RIF, inclusiv documentele de configurare, specificațiile tehnice de interoperabilitate, schemele de date, specificațiile de interfață, regulile tehnice de validare, documentele privind administrarea rolurilor și a profilurilor de acces, precum și documentele privind incidentele de securitate, măsurile de remediere și continuitatea funcționării SI RIF, care se elaborează, se aprobă, se actualizează și se păstrează în conformitate cu cadrul normativ și cu caietul de sarcini al SI RIF.

Capitolul VII
CONȚINUTUL INFORMAȚIONAL AL RIF ȘI UTILIZAREA IDENTIFICATORILOR

Secțiunea 1
Obiectele informaționale gestionate în RIF și utilizarea identificatorilor

54. Conținutul informațional al RIF este constituit din totalitatea obiectelor informaționale, a atributelor, a metadatelor și a identificatorilor utilizați pentru evidența, prelucrarea, compararea, validarea, schimbul automatizat transfrontalier de date și utilizarea imaginilor faciale și a datelor de referință

privind imaginile faciale prin intermediul SI RIF, în condițiile prevăzute de actele normative.

55. Obiectele informaționale de bază gestionate în RIF sunt următoarele:

55.1. imaginea facială identificată;

55.2. imaginea facială neidentificată;

55.3. datele de referință privind imaginea facială;

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

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

55.6. rezultatul comparării automatizate;

55.7. lista mostrelor pentru care există posibilitatea unor concordanțe;

55.8. înregistrarea privind confirmarea sau infirmarea concordanței;

55.9. metadatele aferente obiectelor informaționale gestionate în RIF.

56. Obiectele informaționale proprii ale RIF sunt obiectele prevăzute la subpct. 55.1-55.9, create, gestionate și actualizate în RIF prin intermediul SI RIF, în scopurile prevăzute de Regulamentul privind modul de ținere a Registrului imaginilor faciale.

57. Pentru ținerea RIF pot fi utilizate, prin intermediul SI RIF și al mecanismelor de interoperabilitate, obiecte informaționale preluate din alte sisteme informaționale și resurse informaționale de stat, fără înregistrarea repetată a acestora în RIF, după cum urmează:

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

57.2. unitatea de drept, inclusiv autoritatea sau entitatea furnizoare/destinatară a datelor – din Registrul de stat al unităților de drept sau alte resurse informaționale prevăzute de actele normative, identificată prin IDNO, după caz;

57.3. 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;

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

58. Obiectele informaționale preluate nu constituie obiecte primare de evidență ale RIF și nu se înregistrează în mod repetat în RIF. Pentru ținerea RIF se păstrează, după caz, numai identificatorii obiectelor preluate, datele minime

necesare corelării acestora, metadatele privind sursa datelor, precum și informațiile necesare asigurării trasabilității accesării sau utilizării acestora. Datele aferente obiectelor informaționale împrumutate se consultă sau se consumă, după caz, prin intermediul SI RIF și al mecanismelor de interoperabilitate, în volumul minim necesar realizării scopului legal, fără constituirea în RIF a unei evidențe primare paralele privind persoanele, cauzele, dosarele sau alte obiecte informaționale deja înregistrate în sistemele-sursă.

59. Fiecare obiect informațional propriu gestionat în RIF este identificat în mod unic printr-un identificator atribuit în cadrul RIF, iar obiectele informaționale împrumutate sunt identificate prin identificatorii atribuiți în sistemele informaționale sau resursele informaționale-sursă, cu respectarea interdicției de a înregistra repetat obiectele deja înregistrate în alte registre de stat.

60. Identificatorii principali utilizați pentru obiectele informaționale gestionate în RIF sunt următorii:

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

60.2. pentru imaginea facială neidentificată – numărul de referință al imaginii faciale, identificatorul intern al înregistrării în 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;

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

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

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

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

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

60.8. pentru obiectele informaționale împrumutate – identificatorii atribuiți acestora în sistemele informaționale și resursele informaționale-sursă,

inclusiv IDNP, în cazul persoanei fizice, IDNO, în cazul unității de drept, precum și identificatorul cauzei penale, al dosarului de căutare, al cazului individual sau al altui obiect informațional conex, după caz.

61. Identificatorii obiectelor informaționale gestionate în RIF sunt corelați cu procesele de evidență, comparare, validare, raportare, schimb automatizat transfrontalier de date și arhivare, realizate prin intermediul SI RIF, în condițiile Regulamentului privind modul de ținere a Registrului imaginilor faciale.

62. Identificatorii utilizați pentru obiectele informaționale gestionate în RIF corespund cerințelor cadrului normativ național și, după caz, standardelor și cerințelor tehnice internaționale, astfel încât să fie asigurată interoperabilitatea SI RIF cu alte sisteme informaționale de stat și cu infrastructurile externe utilizate în cadrul cooperării polițienești internaționale.

63. Structura identificatorilor obiectelor informaționale gestionate prin intermediul SI RIF se stabilește după cum urmează:

63.1. numărul de referință al imaginii faciale constituie identificatorul principal al imaginii faciale și include, după caz, următoarele elemente structurale:

63.1.1. codul statului sau al autorității emitente;

63.1.2. codul categoriei obiectului informațional;

63.1.3. identificatorul unic al imaginii faciale;

63.1.4. indicatorul privind caracterul identificat sau neidentificat al imaginii faciale;

63.1.5. elementul de versiune sau de actualizare, după caz;

63.1.6. elementul tehnic de control al integrității identificatorului, după caz;

63.2. identificatorul intern al înregistrării în SI RIF constituie identificatorul tehnic unic atribuit fiecărei înregistrări create în sistem și include, după caz, codul tipului de obiect informațional, codul componentei funcționale în care este creată înregistrarea, marcajul temporal al înregistrării și secvența unică generată de sistem;

63.3. identificatorul datelor de referință privind imaginea facială include numărul de referință al imaginii faciale, codul categoriei setului de date, codul statutului imaginii faciale și elementele tehnice necesare delimitării setului de date de referință destinat schimbului automatizat transfrontalier de componenta națională a RIF;

63.4. identificatorul solicitării de căutare automatizată include codul autorității solicitante, codul statului solicitant, numărul unic al solicitării, data și ora generării acesteia, precum și codul tipului de căutare automatizată;

63.5. identificatorul răspunsului la solicitarea de căutare automatizată include codul autorității respondente, codul statului respondent, numărul unic al

răspunsului, data și ora generării răspunsului și numărul solicitării la care se referă;

63.6. identificatorul rezultatului comparării automatizate include numărul unic al rezultatului comparării, numărul de referință al imaginii faciale supuse comparării, numărul de referință al mostrei comparative sau al mostrelor comparative relevante, după caz, tipul comparării și marcajul temporal al generării rezultatului;

63.7. identificatorul listei mostrelor pentru care există posibilitatea unei concordanțe include numărul unic al listei, identificatorul rezultatului comparării automatizate, numărul de referință al imaginii faciale supuse comparării, data și ora generării listei și indicatorul statutului acesteia;

63.8. identificatorul înregistrării privind confirmarea sau infirmarea concordanței include identificatorul unic al validării, identificatorul rezultatului comparării automatizate, identificatorul utilizatorului care a efectuat validarea, data și ora validării, precum și indicatorul rezultatului validării;

63.9. identificatorii obiectelor informaționale împrumutate sunt cei atribuiți acestora în sistemele informaționale și resursele informaționale-sursă, inclusiv IDNP, în cazul persoanei fizice, IDNO, în cazul unității de drept, precum și identificatorul cauzei penale, al dosarului de căutare, al cazului individual sau al altui obiect informațional conex, după caz;

63.10. identificatorii prevăzuți la subpct. 63.1-63.9 se generează, se utilizează, se corelează și se păstrează astfel încât să se asigure unicitatea identificării obiectelor informaționale, trasabilitatea operațiunilor, interoperabilitatea cu sistemele informaționale și resursele informaționale-sursă, precum și delimitarea obiectelor informaționale proprii ale SI RIF de obiectele informaționale preluate;

63.11. formatul tehnic, lungimea câmpurilor, regulile de codificare, regulile de validare, algoritmii de generare și elementele tehnice de control ale identificatorilor se detaliază în documentația tehnică aferentă SI RIF, cu respectarea structurii logice prevăzute de prezentul Concept și a cadrului normativ în domeniul registrelor, al resurselor informaționale de stat, al interoperabilității și al securității informației.

Secțiunea a 2-a
Atributele obiectelor informaționale gestionate în RIF

64. Atributele obiectelor informaționale gestionate în RIF includ:

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

64.1.1. numărul de referință;

64.1.2. identificatorul intern al înregistrării;

64.1.3. statutul imaginii faciale;

64.1.4. imaginea facială;

64.1.5. datele privind sursa imaginii faciale;

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

64.1.7. temeiul introducerii imaginii faciale în RIF;

64.1.8. datele privind autoritatea sau entitatea care a introdus imaginea facială în RIF;

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

64.1.10. datele minime de identificare ale persoanei fizice, preluate din sistemul-sursă sau verificate prin intermediul acestuia, strict necesare pentru confirmarea concordanței, identificarea persoanei sau furnizarea informațiilor suplimentare în condițiile prevăzute de actele normative, fără constituirea în RIF a unei evidențe primare a persoanelor;

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

64.1.12. datele privind rezultatul comparării automatizate, după caz;

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

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

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

64.2.1. numărul de referință;

64.2.2. identificatorul intern al înregistrării;

64.2.3. statutul imaginii faciale;

64.2.4. indicatorul caracterului neidentificat al imaginii faciale;

64.2.5. imaginea facială;

64.2.6. datele privind sursa imaginii faciale;

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

64.2.8. temeiul introducerii imaginii faciale în RIF;

64.2.9. datele privind autoritatea sau entitatea care a introdus imaginea facială în RIF;

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

64.2.11. datele privind rezultatul comparării automatizate, după caz;

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

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

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

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

64.3.1. imaginea facială;

64.3.2. numărul de referință;

64.3.3. codul statului care deține imaginea facială;

64.3.4. indicatorul caracterului identificat sau neidentificat al imaginii faciale;

64.3.5. alte metadate strict necesare pentru efectuarea comparării și a schimbului automatizat, care nu permit identificarea directă a persoanei;

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

64.4.1. codul statului solicitant;

64.4.2. data solicitării;

64.4.3. ora solicitării;

64.4.4. numărul solicitării;

64.4.5. datele de referință privind imaginea facială;

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

64.5.1. mențiunea privind existența unei concordanțe, a mai multor concordanțe sau inexistența concordanței;

64.5.2. data solicitării;

64.5.3. ora solicitării;

64.5.4. numărul solicitării;

64.5.5. data răspunsului;

64.5.6. ora răspunsului;

64.5.7. numărul răspunsului;

64.5.8. codul statului solicitant;

64.5.9. codul statului solicitat;

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

64.5.11. imaginile faciale între care a fost stabilită o concordanță;

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

64.6.1. identificatorul rezultatului comparării;

64.6.2. numărul de referință al imaginii faciale supuse comparării;

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

64.6.4. data și ora comparării;

64.6.5. rezultatul comparării;

64.6.6. nivelul de asemănare, după caz;

64.6.7. datele privind componenta sau procesul tehnic prin intermediul căruia a fost generat rezultatul;

64.6.8. statutul rezultatului comparării;

64.7. datele privind obiectul informațional „lista mostrelor pentru care există posibilitatea unei concordanțe”:

64.7.1. identificatorul listei;

64.7.2. identificatorul rezultatului comparării automatizate;

64.7.3. numărul de referință al imaginii faciale supuse comparării;

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

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

64.7.6. ordinea mostrelor în listă;

64.7.7. data și ora formării listei;

64.7.8. statutul listei;

64.8. datele privind obiectul informațional „înregistrarea privind confirmarea sau infirmarea concordanței”:

64.8.1. identificatorul validării;

64.8.2. identificatorul rezultatului comparării;

64.8.3. data și ora validării;

64.8.4. rezultatul validării;

64.8.5. datele privind persoana calificată care a efectuat validarea;

64.8.6. observațiile privind confirmarea sau infirmarea concordanței, după caz;

64.9.datele privind obiectul informațional „metadatele aferente obiectelor informaționale”:

64.9.1. sursa datelor;

64.9.2. data și ora recepționării;

64.9.3. temeiul legal al introducerii;

64.9.4. istoricul actualizărilor;

64.9.5. legătura cu alte obiecte informaționale;

64.9.6. informații privind jurnalizarea și trasabilitatea operațiunilor;

64.9.7. identificatorul obiectului informațional împrumutat și denumirea sistemului informațional sau a resursei informaționale-sursă din care acesta este preluat ori prin intermediul căreia este consultat, după caz.

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

66. Fiecare obiect informațional include în mod obligatoriu atributul „statut”, care indică starea curentă a acestuia, inclusiv, după caz, starea activă, actualizată, blocată, radiată, arhivată sau o altă stare stabilită prin Regulamentul privind modul de ținere a Registrului imaginilor faciale.

67. 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 în documentația tehnică aferentă sistemului.

Secțiunea a 3-a
Nomenclatoarele, clasificatoarele și regulile de validare utilizate în SI RIF

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

69. Nomenclatoarele și clasificatoarele utilizate în cadrul SI RIF includ, după caz:

69.1. clasificatorul autorităților și entităților participante;

69.2. clasificatorul categoriilor de utilizatori și al profilurilor de acces;

69.3. nomenclatorul tipurilor și surselor imaginilor faciale;

69.4. nomenclatorul statutelor imaginilor faciale și al obiectelor informaționale;

69.5. clasificatorul temeiurilor legale de introducere, actualizare, blocare, radiere și arhivare a datelor;

69.6. nomenclatorul tipurilor de obiecte informaționale gestionate în sistem;

69.7. nomenclatorul rezultatelor comparării automatizate;

69.8. nomenclatorul rezultatelor validării concordanței;

69.9. clasificatorul incidentelor de securitate și al măsurilor aplicate;

69.10. clasificatorul motivelor de rectificare, completare, actualizare, blocare, radiere și arhivare a datelor;

69.11. nomenclatorul canalelor și tipurilor de schimb de date;

69.12. clasificatorul codurilor de țară și al altor coduri utilizate în schimbul automatizat transfrontalier al datelor;

69.13. alte nomenclatoare, clasificatoare și tabele de coduri necesare funcționării SI RIF.

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

71. Nomenclatoarele și clasificatoarele utilizate în cadrul SI RIF sunt compatibile, după caz, cu cele utilizate în alte sisteme informaționale și resurse informaționale de stat relevante, în vederea asigurării interoperabilității și a schimbului de date.

72. Regulile de validare aplicabile datelor introduse și procesate în SI RIF asigură:

72.1. verificarea completitudinii datelor obligatorii;

72.2. verificarea corectitudinii formatului datelor;

72.3. verificarea unicității identificatorilor și a numerelor de referință;

72.4. verificarea coerenței logice dintre atributele obiectelor informaționale;

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

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

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

72.8. verificarea îndeplinirii cerințelor minime de calitate a imaginii faciale necesare pentru utilizarea acesteia în procesul de comparare automatizată;

72.9. verificarea corectitudinii datelor utilizate în solicitările de căutare automatizată și în răspunsurile la acestea;

72.10. verificarea corectitudinii datelor transmise sau recepționate prin mecanisme de interoperabilitate cu alte sisteme informaționale.

73. Introducerea și prelucrarea datelor în SI RIF se efectuează numai după validarea acestora în conformitate cu regulile stabilite pentru obiectul informațional respectiv.

74. În cazul constatării unor erori, neconcordanțe, omisiuni sau incompatibilități, SI RIF permite, după caz, respingerea datelor, suspendarea prelucrării acestora, marcarea lor distinctă sau returnarea datelor în vederea completării ori rectificării.

75. Regulile de validare asigură prevenirea introducerii în SI RIF a datelor incomplete, eronate, contradictorii, duplicate sau incompatibile cu structura și scopul sistemului.

76. Structura și conținutul nomenclatoarelor, clasificatoarelor, tabelelor de coduri și ale regulilor de validare, precum și modul de administrare și actualizare a acestora se stabilesc în documentația tehnică aferentă SI RIF.

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

77. SI RIF este găzduit de Platforma tehnologică guvernamentală comună (MCloud), în conformitate cu Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud), și este compatibil cu platforma de găzduire bazată pe tehnologii de tip container, în vederea utilizării eficiente a resurselor.

78. Pentru schimbul de date și asigurarea interoperabilității cu alte sisteme informaționale și resurse informaționale de stat, SI RIF interacționează prin intermediul platformei guvernamentale de interoperabilitate (MConnect), inclusiv, după caz, prin utilizarea componentei MConnect Events și a interfețelor de programare a aplicațiilor (API), în vederea expunerii și consumului evenimentelor de sistem relevante pentru interoperabilitate, cu respectarea cadrului normativ, a cerințelor tehnice stabilite de Instituția publică ,,Agenția de

Guvernare Electronică”, a cerințelor de securitate și a documentației tehnice aferente SI RIF, precum și cu următoarele sisteme informaționale partajate:

78.1.serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea utilizatorilor și controlul accesului la SI RIF;

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

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

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

79. SI RIF interacționează cu următoarele sisteme informaționale și resurse informaționale de stat relevante, în vederea consumului, furnizării și corelării următoarelor categorii de date:

79.1. Sistemul informațional automatizat „Registrul informației criminalistice și criminologice” – pentru consumul, verificarea și corelarea datelor privind cauza penală, cazul individual, persoanele vizate în cadrul procedurilor penale, calitatea procesuală sau statutul juridic relevant, infracțiunea ori fapta investigată, identificatorii cauzei, ai dosarului sau ai altor obiecte informaționale conexe, precum și a altor date necesare pentru confirmarea temeiului legal al introducerii, actualizării, utilizării sau radierii datelor din RIF;

79.2. Sistemul informațional automatizat „Registrul dactiloscopic” – pentru consumul, verificarea și corelarea datelor privind persoanele înregistrate dactiloscopic, identificatorii înregistrărilor dactiloscopice, datele de identificare ale persoanei, datele privind temeiul înregistrării dactiloscopice, legătura cu cauza penală, dosarul ori cazul individual și alte date necesare corelării obiectelor informaționale gestionate în RIF cu evidențele dactiloscopice;

79.3. Sistemul informațional „Registrul de stat al populației” – pentru consumul, verificarea și corelarea datelor de identificare ale persoanei fizice, inclusiv IDNP, numele, prenumele, data nașterii, sexul, cetățenia, datele privind actele de identitate, statutul persoanei, datele privind imaginea facială disponibilă în sistemul-sursă, precum și alte date strict necesare identificării persoanei și corelării imaginii faciale cu persoana fizică luată la evidență;

79.4. Sistemul informațional al Inspectoratului General al Poliției de Frontieră – pentru consumul, verificarea și corelarea datelor privind persoanele și documentele de călătorie verificate în cadrul atribuțiilor Poliției de Frontieră, evenimentele relevante de frontieră, imaginile faciale ori materialele foto-video obținute în condițiile actelor normative, identificatorii operațiunilor de control, ai cazurilor ori ai dosarelor conexe, precum și alte date necesare realizării atribuțiilor privind prevenirea, constatarea și investigarea infracțiunilor, căutarea persoanelor și cooperarea polițienească internațională;

79.5. Sistemul informațional al Inspectoratului General pentru Migrație – pentru consumul, verificarea și corelarea datelor privind străinii, apatrizii, solicitanții de azil, beneficiarii unei forme de protecție, persoanele documentate în proceduri migraționale, actele eliberate sau procedurile aferente acestora, imaginile faciale disponibile în sistemele-sursă, identificatorii dosarelor migraționale și alte date necesare identificării persoanei și realizării atribuțiilor legale ale autorităților competente;

79.6. alte sisteme informaționale și resurse informaționale de stat, stabilite de cadrul normativ – pentru consumul, furnizarea și corelarea datelor strict necesare formării, actualizării, verificării, utilizării, validării, radierii, arhivării și auditării datelor gestionate în RIF, în limitele scopului legal și ale necesității funcționale documentate.

80. Interacțiunea cu sistemele informaționale prevăzute la pct. 79 se realizează exclusiv în scopul formării, actualizării, verificării, utilizării și validării datelor gestionate prin intermediul SI RIF, precum și al asigurării schimbului de date în condițiile prevăzute de actele normative. În cadrul acestei interacțiuni pot fi preluate sau furnizate, după caz și în limita necesității funcționale documentate, următoarele categorii de date:

80.1. imaginile faciale și datele de referință privind imaginile faciale, în cazurile prevăzute de actele normative;

80.2. metadatele aferente imaginilor faciale, inclusiv datele privind sursa, data, temeiul și contextul obținerii acestora;

80.3. identificatorii tehnici, numerele de referință, codurile și alte date necesare corelării obiectelor informaționale;

80.4. datele necesare verificării identității persoanei sau corelării acesteia cu cazul individual, cauza penală, dosarul de căutare ori cu un alt obiect informațional relevant;

80.5. rezultatele comparării automatizate, listele mostrelor pentru care există posibilitatea unei concordanțe și înregistrările privind confirmarea sau infirmarea concordanței;

80.6. datele privind jurnalizarea, auditul și trasabilitatea, în limitele necesare verificării legalității accesului la date și a schimbului de date.

81. În cazul în care legislația prevede necesitatea deținerii unor date sau documente disponibile în resursele informaționale ale altor autorități publice pentru introducerea, actualizarea sau utilizarea datelor în RIF, acestea pot fi preluate sau furnizate prin intermediul platformei de interoperabilitate (MConnect).

82. La nivel internațional, SI RIF contribuie la:

82.1. realizarea schimbului automatizat transfrontalier de date de referință privind imaginile faciale, în conformitate cu cadrul normativ național în

domeniul cooperării polițienești internaționale, cu tratatele internaționale la care Republica Moldova este parte și cu actele de punere în aplicare a acestora;

82.2. furnizarea, ulterior confirmării unei concordanțe, a datelor de bază și a informațiilor suplimentare, în conformitate cu cadrul normativ național în domeniul cooperării polițienești internaționale, cu tratatele internaționale la care Republica Moldova este parte și cu actele de punere în aplicare a acestora;

82.3. interacțiunea cu infrastructurile și mecanismele externe utilizate în cadrul cooperării polițienești internaționale, în conformitate cu cadrul normativ național în domeniul cooperării polițienești internaționale, de tratatele internaționale la care Republica Moldova este parte și ale actelor de punere în aplicare ale acestora;

82.4. aplicarea măsurilor de securitate, confidențialitate și trasabilitate în cadrul transmiterii transfrontaliere a datelor.

83. Schimbul de date dintre SI RIF și alte sisteme informaționale se realizează cu respectarea următoarelor principii:

83.1. legalitatea – schimbul de date se realizează numai în temeiul și în limitele prevăzute de lege;

83.2. securitatea – datele sunt protejate împotriva accesului neautorizat, precum și împotriva altor riscuri de securitate;

83.3. trasabilitatea – fiecare acces la date și fiecare transfer de date se înregistrează și poate fi verificat ulterior;

83.4. proporționalitatea – se transmit numai datele necesare și relevante pentru realizarea scopului urmărit;

83.5. interoperabilitatea – schimbul de date se realizează prin mecanisme compatibile din punct de vedere juridic, organizatoric, semantic și tehnic;

83.6. reciprocitatea – schimbul de date cu entitățile externe se realizează în condițiile prevăzute de tratatele internaționale la care Republica Moldova este parte.

84. Subiecții care participă la formarea și actualizarea RIF prin preluarea sau furnizarea datelor prin intermediul mecanismelor de interoperabilitate sunt autoritățile și entitățile publice care dețin sau administrează sisteme informaționale și resurse informaționale relevante, în limitele competențelor stabilite prin actele normative.

85. 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.

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

Secțiunea a 5-a
Scenariile de bază utilizate în SI RIF

87. Scenariile de bază utilizate în SI RIF descriu principalele fluxuri funcționale și informaționale prin care se realizează alimentarea, administrarea, compararea, validarea, utilizarea și schimbul automatizat transfrontalier al imaginilor faciale și al datelor de referință privind acestea.

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

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

88.2. verificarea formală și tehnică a datelor recepționate;

88.3. atribuirea numărului de referință;

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

88.5. înregistrarea datelor și a metadatelor aferente în RIF.

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

89.1. actualizarea, rectificarea și completarea datelor introduse în SI RIF;

89.2. modificarea statutului obiectelor informaționale, după caz;

89.3. blocarea, radierea și arhivarea datelor;

89.4. păstrarea informațiilor privind temeiul legal al operațiunii, istoricului actualizărilor și, după caz, rezultatul comparării automatizate, precum și confirmarea sau infirmarea concordanței.

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

90.1. colectarea și centralizarea mostrelor comparative din surse autorizate;

90.2. asocierea mostrelor pentru comparație cu metadatele sau identificatorii necesari pentru desfășurarea procesului de identificare;

90.3. actualizarea și utilizarea repozitoriului în procesul de comparare automatizată.

91. Scenariul de bază privind compararea automatizată a datelor de referință referitoare la imaginile faciale presupune:

91.1. inițierea unei solicitări de comparare aferente unui caz individual;

91.2. compararea automatizată a imaginii faciale cu mostrele disponibile, inclusiv prin aplicarea algoritmului de comparare de tip 1:1 și 1:N;

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

91.4. generarea rezultatului tehnic preliminar al comparării și, după caz, întocmirea listei mostrelor pentru care există posibilitatea unei concordanțe, fără ca includerea unei mostre în această listă să constituie o confirmare înainte de validarea acesteia de către personalul calificat.

92. Scenariul de bază privind sprijinirea identificării cazului sau a persoanei presupune:

92.1. extragerea și structurarea datelor de bază și a informațiilor suplimentare necesare pentru identificarea persoanei și, după caz, pentru individualizarea cazului;

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

92.3. furnizarea datelor necesare autorităților competente.

93. Scenariul de bază privind validarea concordanței presupune:

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

93.2. confirmarea sau infirmarea concordanței;

93.3. înregistrarea rezultatului validării și păstrarea acestuia în SI RIF.

94. Scenariul de bază privind căutarea și schimbul automatizat transfrontalier de date presupune:

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

94.2. recepționarea și prelucrarea solicitării de căutare automatizată a datelor de referință privind imaginile faciale;

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

94.4. furnizarea, după caz, a datelor de bază și a informațiilor suplimentare ulterior confirmării unei concordanțe.

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

95.1. preluarea și furnizarea datelor prin intermediul platformei de interoperabilitate (MConnect);

95.2. preluarea datelor și a metadatelor din sistemele-sursă relevante;

95.3. utilizarea serviciilor guvernamentale partajate pentru autentificare, jurnalizare, semnare electronică, notificare și pentru asigurarea altor funcționalități necesare exploatării SI RIF;

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

96. Scenariul de bază privind interacțiunea cu infrastructurile informaționale externe utilizate în cadrul cooperării polițienești internaționale presupune:

96.1. pregătirea și extragerea seturilor de date necesare;

96.2. transmiterea și recepționarea datelor în conformitate cu cadrul normativ național în domeniul cooperării polițienești internaționale, cu tratatele internaționale la care Republica Moldova este parte și cu actele de punere în aplicare a acestora;

96.3. aplicarea măsurilor de asigurare a confidențialității, integrității și protecției datelor cu caracter personal, precum și a măsurilor de criptare și jurnalizare;

96.4. utilizarea rezultatelor schimbului automatizat transfrontalier de date în conformitate cu cadrul normativ național în domeniul cooperării polițienești internaționale, cu tratatele internaționale la care Republica Moldova este parte și cu actele de punere în aplicare a acestora.

97. Scenariul de bază privind administrarea, controlul și auditul SI RIF presupune:

97.1. administrarea utilizatorilor, a rolurilor și a profilurilor de acces;

97.2. jurnalizarea operațiunilor efectuate în SI RIF;

97.3. monitorizarea și controlul utilizării SI RIF;

97.4. gestionarea incidentelor de securitate;

97.5. auditarea și verificarea trasabilității operațiunilor.

Capitolul VIII
STRUCTURA INFORMAȚIONALĂ ȘI TEHNOLOGICĂ A SI RIF

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

99. Structura informațională a SI RIF include următoarele componente:

99.1. RIF, ca resursă informațională departamentală de stat specializată, ținută în format electronic;

99.2. obiectele informaționale și atributele acestora;

99.3. datele de referință privind imaginile faciale;

99.4. metadatele aferente obiectelor informaționale;

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

99.6. evidențele privind solicitările de căutare automatizată și răspunsurile la acestea;

99.7. evidențele privind rezultatele comparării automatizate și validarea concordanței;

99.8. jurnalele operațiunilor și alte evidențe necesare pentru asigurarea trasabilității și a controlului utilizării SI RIF.

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

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

101.1. componenta de stocare și administrare a datelor;

101.2. componenta de comparare biometrică a imaginilor faciale;

101.3. componenta de sprijinire a identificării cazului sau a persoanei;

101.4. componenta de validare a concordanței;

101.5. componenta de interoperabilitate și schimb de date;

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

101.7. componenta de jurnalizare, monitorizare și audit;

101.8. componenta de securitate și protecție a datelor;

101.9. componenta de raportare și valorificare a datelor.

102. Componenta de stocare și administrare a datelor asigură evidența, păstrarea, actualizarea, rectificarea, completarea, blocarea, radierea și arhivarea obiectelor informaționale gestionate în SI RIF.

103. Componenta de comparare biometrică a imaginilor faciale asigură compararea automatizată a imaginilor faciale cu mostrele disponibile pentru comparație, inclusiv prin aplicarea mecanismelor de tip 1:1 și 1:N, precum și generarea rezultatului comparării.

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

105. Componenta de validare a concordanței asigură examinarea de către personalul calificat a rezultatelor comparării automatizate, precum și înregistrarea confirmării sau infirmării concordanței.

106. 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 cadrul cooperării polițienești internaționale, în conformitate cu cadrul normativ național, cu tratatele internaționale la care Republica Moldova este parte și cu actele de punere în aplicare a acestora.

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

108. Componenta de jurnalizare, monitorizare și audit asigură evidența operațiunilor efectuate în SI RIF, trasabilitatea prelucrării datelor, monitorizarea utilizării SI RIF, precum și suportul necesar pentru efectuarea controlului intern și a auditului.

109. Componenta de securitate și protecție a datelor asigură aplicarea măsurilor tehnice și organizatorice necesare pentru garantarea confidențialității, integrității, disponibilității și autenticității datelor, precum și pentru asigurarea rezilienței SI RIF.

110. SI RIF utilizează, după caz, sisteme informaționale partajate și servicii guvernamentale comune pentru autentificare, semnare electronică, jurnalizare, notificare, schimb de date și găzduire, în conformitate cu cadrul normativ.

111. 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 în domeniul schimbului de date, al interoperabilității, al protecției datelor cu caracter personal și al securității informației.

112. Structura informațională și tehnologică a SI RIF asigură:

112.1. integritatea și coerența datelor;

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

112.3. accesul autorizat și diferențiat;

112.4. jurnalizarea și trasabilitatea operațiunilor;

112.5. protecția datelor cu caracter personal și securitatea informației;

112.6. posibilitatea dezvoltării și extinderii ulterioare a SI RIF.

113. Soluțiile tehnice utilizate în cadrul SI RIF permit implementarea funcționalităților prevăzute de cadrul normativ național în domeniul cooperării polițienești internaționale și de actele de punere în aplicare a acestora, în ceea ce privește imaginile faciale, inclusiv a cerințelor privind datele de referință, solicitările și răspunsurile automatizate, utilizarea în cazuri individuale, jurnalizarea, trasabilitatea, securitatea, precum și furnizarea ulterioară a datelor de bază și a informațiilor suplimentare după confirmarea concordanței.

114. Structura detaliată a componentelor informaționale și tehnologice, cerințele funcționale și nefuncționale, mecanismele de integrare, modelele și formatele de date, protocoalele de comunicare și de schimb de date, regulile tehnice de validare, precum și mecanismele de securitate, jurnalizare, trasabilitate, disponibilitate și continuitate, inclusiv cele aferente componentei de schimb automatizat transfrontalier de date de referință privind imaginile faciale, se stabilesc în documentația tehnică a SI RIF, cu respectarea cadrului normativ și a standardelor europene și internaționale.

Capitolul IX
ASIGURAREA SECURITĂȚII INFORMAȚIONALE A SI RIF

115. Asigurarea securității informaționale a SI RIF cuprinde ansamblul măsurilor juridice, organizatorice, economice și tehnologice orientate spre prevenirea și diminuarea riscurilor de securitate aferente resurselor informaționale, componentelor funcționale și infrastructurii tehnologice a sistemului.

116. Securitatea informațională presupune protecția SI RIF în toate etapele de colectare, recepționare, prelucrare, comparare, validare, stocare, utilizare și transmitere a datelor împotriva acțiunilor intenționate sau accidentale, cu caracter artificial ori natural, care pot cauza prejudicii utilizatorilor sistemului ori pot afecta datele prelucrate și infrastructura informațională.

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

118. Principalele amenințări pentru securitatea informațională a SI RIF sunt următoarele:

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

118.2. compromiterea, perturbarea ori utilizarea neautorizată a proceselor și mecanismelor tehnologice de selectare, comparare, validare, prelucrare și schimb de date;

118.3. implementarea în produsele software a unor componente care îndeplinesc funcții neprevăzute în documentația tehnică;

118.4. elaborarea, distribuirea sau utilizarea programelor informatice care afectează funcționarea normală a SI RIF;

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

118.6. scurgerea informației prin canale tehnice;

118.7. interceptarea informațiilor transmise prin rețelele de transmitere a datelor și liniile de comunicații, decriptarea neautorizată a acestora sau introducerea de informații false;

118.8. distrugerea, deteriorarea, modificarea, blocarea sau sustragerea suporturilor și resurselor informaționale;

118.9. utilizarea tehnologiilor, aplicațiilor sau mijloacelor de protecție necorespunzătoare ori necertificate, în cazurile în care certificarea este obligatorie potrivit legii;

118.10. încălcarea prevederilor legislației în domeniul protecției datelor cu caracter personal, al securității informației și al securității cibernetice;

118.11. accesul neautorizat la jurnalele operațiunilor, rezultatele comparării automatizate, înregistrările privind validarea concordanței sau la alte date sensibile generate de sistem.

119. SI RIF asigură îndeplinirea următoarelor obiective de securitate:

119.1. autentificarea – asigură verificarea identității utilizatorilor și permite accesul la zonele cu acces restricționat ale sistemului numai utilizatorilor autorizați, inclusiv prin utilizarea, după caz, a serviciului electronic guvernamental de autentificare și control al accesului (MPass);

119.2. confidențialitatea – asigură protecția imaginilor faciale, a datelor de referință și a celorlalte date gestionate în sistem împotriva accesului neautorizat;

119.3. integritatea – asigură protecția datelor gestionate în sistem împotriva modificării, alterării sau distrugerii neautorizate;

119.4. disponibilitatea – asigură accesibilitatea datelor și a funcționalităților sistemului pentru utilizatorii autorizați atunci când este necesar;

119.5. nerepudierea – asigură posibilitatea de a demonstra efectuarea operațiunilor în sistem și de a identifica autorii acestora, astfel încât aceștia să nu poată nega ulterior efectuarea operațiunilor respective;

119.6. trasabilitatea – asigură posibilitatea urmăririi și verificării ulterioare a fiecărei accesări și a fiecărei operațiuni relevante efectuate în SI RIF.

120. Pentru asigurarea unui nivel adecvat de securitate informațională a SI RIF, deținătorul SI RIF elaborează și implementează politica de securitate informațională, aprobată de posesorul SI RIF, prin care se stabilesc măsurile de securitate, rolurile, drepturile și obligațiile subiecților sistemului, precum și procedurile de control al accesului, de jurnalizare, de răspuns la incidente, de asigurare a continuității și de recuperare a datelor.

121. Un element esențial al securității informaționale îl constituie păstrarea înregistrărilor de audit necesare pentru verificarea 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), pentru asigurarea evidenței operațiunilor și a trasabilității activităților desfășurate în sistem.

122. În scopul asigurării interoperabilității și a schimbului de date cu alte sisteme și resurse informaționale de stat, activele semantice utilizate în SI RIF se înregistrează în Sistemul informațional „Catalogul semantic” și se utilizează în conformitate cu 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”.

Capitolul X
ÎNCHEIERE

123. Prezentul Concept descrie principalele aspecte organizatorice, metodologice, funcționale, informaționale și tehnologice care stau la baza conceperii și implementării SI RIF, ca soluție informațională specializată, destinată să asigure suportul informațional necesar autorităților competente în procesele de colectare, evidență, comparare, validare, utilizare și schimb automatizat transfrontalier de date de referință privind imaginile faciale.

124. Prezentul Concept stabilește cadrul general pentru crearea, dezvoltarea și funcționarea 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 privind interoperabilitatea, protecția datelor cu caracter personal, securitatea informațională, precum și nivelului actual de dezvoltare a infrastructurii digitale a Republicii Moldova.

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

125.1. asigurarea unei evidențe unice, structurate și fiabile a imaginilor faciale și a datelor de referință privind imaginile faciale;

125.2. consolidarea capacităților autorităților competente în domeniul prevenirii, constatării și investigării infracțiunilor, al identificării persoanelor și al cooperării polițienești internaționale;

125.3. asigurarea comparării automatizate a imaginilor faciale, validarea concordanțelor și furnizarea, în condițiile prevăzute de cadrul normativ, a datelor de bază și a informațiilor suplimentare;

125.4. sporirea nivelului de interoperabilitate cu alte sisteme informaționale și resurse informaționale relevante ale statului;

125.5. facilitarea schimbului automatizat transfrontalier de date, cu respectarea cerințelor de legalitate, securitate, trasabilitate și protecție a datelor cu caracter personal;

125.6. crearea premiselor tehnice și organizatorice necesare alinierii progresive la cerințele europene aplicabile în domeniul căutării și schimbului automatizat transfrontalier de date în scopul cooperării polițienești, în partea ce privește imaginile faciale.

Anexa nr. 2
la Hotărârea Guvernului nr. /2026

REGULAMENT
privind modul de ținere a Registrului imaginilor faciale

Capitolul I
DISPOZIȚII GENERALE

1. Regulamentul privind modul de ținere a Registrului imaginilor faciale (denumit în continuare *Regulament*) stabilește modul de organizare, ținere, administrare, actualizare, utilizare, furnizare, protecție și arhivare a datelor din Registrul imaginilor faciale (denumit în continuare *RIF*), ținut prin intermediul Sistemului informațional „Registrul imaginilor faciale” (denumit 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 transfrontalier de date de referință privind imaginile faciale.

2. Prezentul Regulament stabilește drepturile și obligațiile subiecților raporturilor juridice aferente ținerii RIF, categoriile de date gestionate, modul 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 RIF.

4. RIF constituie o 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 tratatele internaționale la care

Republica Moldova este parte și cu actele normative în domeniul cooperării polițienești internaționale.

6. Termenii și noțiunile utilizate în prezentul Regulament au semnificațiile prevăzute de legislația în domeniul informatizării și al resurselor informaționale de stat, al registrelor de stat, al schimbului de date și al interoperabilității, al protecției datelor cu caracter personal și al securității cibernetice, de actele normative și tratatele internaționale în domeniul cooperării polițienești internaționale, precum și de Conceptul Sistemului informațional „Registrul imaginilor faciale”.

7. Înscrierile, evidențele, metadatele, jurnalele, informațiile și documentele generate sau administrate în cadrul RIF se întocmesc și se administrează în limba română, cu excepția codurilor, identificatorilor, mesajelor și denumirilor tehnice, precum și a informațiilor recepționate sau transmise în cadrul cooperării internaționale, care se păstrează în forma în care au fost recepționate sau în formatul stabilit prin documentația tehnică a SI RIF.

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 prevăzute de actele normative, în limitele competențelor atribuite, cu asigurarea jurnalizării și trasabilității operațiunii, precum și a posibilității de verificare și auditare a utilizării datelor.

Capitolul II
SUBIECȚII RAPORTURILOR JURIDICE AFERENTE ȚINERII RIF ȘI ADMINISTRĂRII SI RIF

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

9.1. proprietarul SI RIF și al RIF;
9.2. posesorul SI RIF și al RIF;
9.3. deținătorul SI RIF;
9.4. registratorii datelor în RIF;
9.5. furnizorii de date pentru RIF;
9.6. destinatarii datelor din RIF.

10. Statutul funcțional al subiecților prevăzuți la pct. 9, precum și rolurile acestora în procesele de creare, dezvoltare, administrare și utilizare a SI RIF și de ținere a RIF sunt stabilite în Conceptul Sistemului informațional „Registrul imaginilor faciale”.

11. Drepturile, obligațiile, responsabilitățile, condițiile de acces și modul de exercitare a atribuțiilor subiecților prevăzuți la pct. 9 sunt stabilite prin prezentul Regulament, prin actele normative și administrative emise în executarea acestora.

12. Subiecții prevăzuți la pct. 9 participă la ținerea RIF și la utilizarea SI RIF numai în limitele competențelor stabilite prin actele normative, în baza rolurilor și profilurilor de acces aprobate, cu respectarea principiilor legalității, necesității, proporționalității, limitării scopului și a cerințelor privind securitatea informației, protecția datelor cu caracter personal, jurnalizarea și trasabilitatea operațiunilor.

13. Desemnarea utilizatorilor SI RIF, a registratorilor datelor în RIF, a furnizorilor de date pentru RIF și a destinatarilor datelor din RIF se efectuează de către autoritățile și instituțiile competente, în condițiile prezentului Regulament și ale actelor administrative aprobate de posesorul SI RIF și al RIF.

14. Accesul la SI RIF și la datele din RIF se acordă individual, în funcție de necesitățile de serviciu, de atribuțiile exercitate și de profilul de acces aprobat, fără a conferi drepturi de acces general, de explorare nejustificată a datelor sau de utilizare a acestora în scopuri nedeterminate.

15. Operațiunile asupra datelor din RIF se efectuează prin intermediul SI RIF de către utilizatori autorizați, desemnați de subiecții prevăzuți la pct. 9, în limitele competențelor stabilite prin lege și ale rolurilor de acces aprobate.

16. Furnizarea datelor pentru RIF și accesarea datelor din RIF se realizează prin intermediul mecanismelor de interoperabilitate, al interfețelor și al canalelor autorizate, în condițiile prezentului Regulament și ale actelor normative.

17. Participarea subiecților la schimbul automatizat transfrontalier de date se realizează numai în cazuri individuale, în conformitate cu cadrul normativ național în domeniul cooperării polițienești internaționale, cu tratatele internaționale la care Republica Moldova este parte și cu actele de punere în aplicare a acestora.

18. Subiecții prevăzuți la pct. 9 sunt obligați să asigure exactitatea, actualitatea, relevanța, integritatea, confidențialitatea și securitatea datelor prelucrate, în limitele atribuțiilor și responsabilităților care le revin.

19. Orice operațiune de accesare, introducere, actualizare, rectificare, completare, blocare, radiere, arhivare, comparare, validare, furnizare sau utilizare

a datelor din RIF se efectuează numai în scopurile prevăzute de actele normative și cu respectarea cerințelor de jurnalizare, monitorizare, control și audit.

Capitolul III
DREPTURILE ȘI OBLIGAȚIILE SUBIECȚILOR RAPORTURILOR JURIDICE PRIVIND ȚINEREA RIF ȘI ADMINISTRAREA SI RIF

Secțiunea 1
Drepturile și obligațiile posesorului SI RIF și al RIF

20. Posesorul SI RIF și al RIF este Ministerul Afacerilor Interne, care exercită următoarele drepturi:

20.1. să stabilească cerințele funcționale, organizaționale și de securitate aplicabile ținerii RIF și administrării SI RIF;

20.2. să aprobe regulile interne privind administrarea accesului, rolurile și profilurile de acces ale utilizatorilor, cu asigurarea documentării acestora, comunicării către utilizatorii vizați și punerii la dispoziția autorităților competente de control și supraveghere, în limitele competențelor legale și cu respectarea cerințelor de securitate a informației;

20.3. să solicite deținătorului SI RIF, registratorilor, furnizorilor de date și destinatarilor datelor adoptarea măsurilor necesare pentru ținerea RIF în conformitate cu prevederile legale și pentru funcționarea în condiții de securitate a SI RIF;

20.4. să inițieze măsuri de dezvoltare și modernizare a SI RIF și de asigurare a interoperabilității acestuia, în scopul ținerii RIF și al utilizării datelor din acesta;

20.5. să coordoneze, la nivel instituțional, participarea SI RIF la mecanismul de căutare și schimb automatizat transfrontalier de date de referință privind imaginile faciale.

21. Posesorul SI RIF și al RIF are următoarele obligații:

21.1. să asigure condițiile juridice, financiare și organizatorice necesare pentru crearea, administrarea, mentenanța și dezvoltarea SI RIF, precum și pentru ținerea RIF;

21.2. să organizeze și să coordoneze, în limitele competențelor stabilite de lege, activitatea subiecților implicați în ținerea RIF și administrarea SI RIF;

21.3. să aprobe procedurile interne privind utilizarea datelor din RIF prin intermediul SI RIF, administrarea accesului, validarea concordanțelor, jurnalizarea și auditul;

21.4. să asigure utilizarea datelor din RIF și a componentei de schimb automatizat transfrontalier de date prin intermediul SI RIF numai în scopurile și în condițiile prevăzute de actele normative;

21.5. să asigure, prin intermediul mecanismelor de interoperabilitate, comunicare și notificare prevăzute de prezentul Regulament, de Legea nr. 195/2024 privind protecția datelor cu caracter personal și de celelalte acte normative aplicabile, notificarea autorităților și subiecților competenți, după caz, cu privire la conținutul bazei naționale de date privind imaginile faciale, condițiile tehnice și juridice ale căutărilor automatizate, lista autorităților autorizate și profilurile de acces ale personalului autorizat, precum și actualizarea acestor informații;

21.6. să monitorizeze implementarea SI RIF, ținerea RIF și funcționarea SI RIF, inclusiv în ceea ce privește componenta de schimb automatizat transfrontalier de date;

21.7. să dispună măsuri de remediere în cazul constatării unor deficiențe, incidente de securitate sau situații de utilizare neconformă a datelor din RIF ori a SI RIF;

21.8. să asigure cooperarea interinstituțională necesară ținerii RIF, funcționării SI RIF și asigurării interoperabilității acestuia cu alte sisteme informaționale și resurse informaționale relevante.

Secțiunea a 2-a
Drepturile și obligațiile deținătorului SI RIF

22. Deținătorul SI RIF este Serviciul Tehnologii Informaționale din subordinea Ministerului Afacerilor Interne, care exercită următoarele drepturi:

22.1. să administreze și să asigure exploatarea tehnică a SI RIF, în limitele competențelor și atribuțiilor stabilite de posesor;

22.2. să solicite subiecților SI RIF respectarea cerințelor tehnice și de securitate necesare funcționării SI RIF;

22.3. să suspende sau să restricționeze, după caz, accesul la SI RIF în cazul producerii unor incidente de securitate, al accesului neautorizat sau al tentativelor de acces neautorizat, al compromiterii datelor, al constatării unor neconformități tehnice grave sau vulnerabilități critice ori al existenței unui risc iminent pentru securitatea, integritatea, confidențialitatea sau disponibilitatea SI RIF și a datelor din RIF, cu informarea imediată a posesorului;

22.4. să efectueze lucrări de mentenanță, actualizare, restabilire a funcționării și dezvoltare a SI RIF.

23. Deținătorul SI RIF are următoarele obligații:

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

23.2. să administreze componentele aplicative ale SI RIF, bazele de date, interfețele și componentele de interoperabilitate aflate în responsabilitatea sa, precum și să asigure administrarea tehnică a aplicațiilor sistemului;

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

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

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

23.6. să asigure, în condițiile prevăzute de actele normative și în limitele competențelor sale, funcționarea tehnică a componentei de schimb automatizat transfrontalier de date, inclusiv conectarea și integrarea tehnică a infrastructurii naționale relevante cu mecanismele și infrastructurile externe utilizate în cadrul cooperării polițienești internaționale;

23.7. să asigure implementarea tehnică a accesului personalului autorizat la infrastructurile utilizate pentru schimbul automatizat transfrontalier de date, în baza deciziilor și a profilurilor de acces aprobate de posesor sau de autoritatea competentă, inclusiv prin asigurarea autentificării, trasabilității accesărilor și a actualizării tehnice a profilurilor de acces;

23.8. să asigure crearea și păstrarea copiilor de rezervă, continuitatea funcționării SI RIF și recuperarea datelor și restabilirea funcționării sistemului în cazul producerii unor incidente;

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

23.10. să asigure suportul tehnic și metodologic necesar subiecților SI RIF.

Secțiunea a 3-a
Drepturile și obligațiile registratorilor datelor în RIF

24. Registratorii datelor în RIF sunt persoanele autorizate din cadrul autorităților și instituțiilor prevăzute în Conceptul Sistemului informațional „Registrul imaginilor faciale”, desemnate în condițiile prezentului Regulament și ale actelor administrative aprobate de către posesorul SI RIF și al RIF.

25. Registratorii au următoarele drepturi:

25.1. să efectueze, prin intermediul SI RIF, operațiuni de introducere, actualizare, rectificare, completare, blocare, radiere și arhivare a datelor din RIF, în limitele rolului și profilului de acces atribuite;

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

25.3. să consulte și să utilizeze datele necesare efectuării operațiunilor de înregistrare și actualizare a datelor din RIF;

25.4. să inițieze, în cazurile prevăzute de actele normative, solicitări de comparare automatizată și să înregistreze rezultatele aferente;

25.5. să solicite furnizorilor de date clarificarea, completarea sau corectarea datelor furnizate.

26. Registratorii au următoarele obligații:

26.1. să efectueze, prin intermediul SI RIF, operațiuni asupra datelor din RIF numai în temeiul legii, în limitele atribuțiilor de serviciu și exclusiv în scopurile prevăzute de cadrul normativ;

26.2. să asigure introducerea, actualizarea și rectificarea datelor în mod complet, exact și în timp util, astfel încât acestea să fie corecte și actualizate;

26.3. să verifice temeiul legal al operațiunilor, existența documentelor și a informațiilor justificative, precum și coerența datelor introduse;

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

26.5. să atribuie numerele de referință și să asigure evidența corectă;

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

26.7. să efectueze operațiuni în cadrul componentei de schimb automatizat transfrontalier de date numai în cazuri individuale, cu respectarea procedurilor de validare, jurnalizare și asigurare a trasabilității;

26.8. să asigure confidențialitatea și protecția datelor cu caracter personal la care au acces;

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

Secțiunea a 4-a
Drepturile și obligațiile furnizorului de date pentru RIF

27. Furnizorii de date pentru RIF sunt instituțiile publice și persoanele juridice de drept public sau privat care, în limitele competențelor stabilite prin lege, transmit date, imagini faciale, metadate sau alte informații necesare formării, completării și actualizării RIF, inclusiv prin intermediul mecanismelor de interoperabilitate, precum și, după caz, constituirii și actualizării setului de date de referință destinat schimbului automatizat transfrontalier de date.

28. Furnizorii de date au următoarele drepturi:

28.1. să furnizeze date, imagini faciale, metadate și alte informații relevante pentru RIF, inclusiv prin intermediul SI RIF sau al mecanismelor de interoperabilitate, după caz, în limitele competențelor stabilite prin lege;

28.2. să solicite rectificarea sau actualizarea datelor furnizate anterior, atunci când constată că acestea sunt inexacte, neactualizate sau nu mai sunt relevante;

28.3. să utilizeze mecanismele de interoperabilitate și canalele autorizate pentru furnizarea datelor, în condițiile prevăzute de actele normative;

28.4. să fie informați cu privire la neconcordanțele sau deficiențele identificate în datele furnizate de aceștia.

29. Furnizorii de date au următoarele obligații:

29.1. să furnizeze date, imagini faciale, metadate și alte informații relevante obținute din surse autorizate, numai în condițiile prevăzute de actele normative;

29.2. să asigure legalitatea furnizării, exactitatea, actualitatea, relevanța, integritatea și, după caz, calitatea imaginilor faciale necesară pentru compararea automatizată, în conformitate cu standardele tehnice și cu documentația tehnică aprobată pentru SI RIF;

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

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

29.5. să utilizeze numai mecanismele de interoperabilitate și canalele autorizate pentru furnizarea datelor către RIF;

29.6. să comunice fără întârziere rectificările, actualizările sau retragerile necesare în cazul în care datele furnizate se dovedesc inexacte, neactualizate ori furnizate fără temei legal;

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

29.8. să transmită imagini faciale și date de referință privind imaginile faciale care corespund cerințelor minime de calitate, integritate, exactitate și utilizabilitate prevăzute de prezentul Regulament, de documentația tehnică a SI RIF și de standardele europene și internaționale, precum și, în cazul schimbului automatizat transfrontalier de date, cerințelor tehnice aplicabile mecanismului Prüm.

Secțiunea a 5-a
Drepturile și obligațiile destinatarilor datelor din RIF

30. Destinatarii datelor din RIF sunt autoritățile publice, instituțiile și alte entități abilitate prin lege să acceseze și să utilizeze datele din RIF, prin intermediul SI RIF sau al altor canale autorizate, în scopul exercitării 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 național în domeniul cooperării polițienești internaționale.

31. Destinatarii datelor din RIF au următoarele drepturi:

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

31.2. să utilizeze datele primite pentru prevenirea, depistarea, constatarea și investigarea infracțiunilor, identificarea ori verificarea identității persoanelor, căutarea persoanelor dispărute, identificarea cadavrelor sau a părților acestora, precum și în alte scopuri prevăzute de actele normative, în legătură cu un caz individual determinat, în baza unui temei juridic documentat și pentru un scop determinat, explicit și legitim;

31.3. să solicite, după caz, extragerea și furnizarea datelor de bază și a informațiilor suplimentare aferente unei concordanțe confirmate, prin intermediul canalelor și punctelor de contact stabilite de cadrul normativ;

31.4. să solicite verificarea, rectificarea sau actualizarea datelor în cazul constatării unor neconcordanțe.

32. Destinatarii datelor din RIF au următoarele obligații:

32.1. să acceseze și să utilizeze datele numai în scopurile și în limitele prevăzute de actele normative;

32.2. să respecte regimul diferențiat de acces la date, în funcție de categoria acestora, de temeiul legal al solicitării și de scopul utilizării lor;

32.3. să nu utilizeze datele pentru efectuarea unor interogări generale sau exploratorii ori în alte scopuri decât cele prevăzute de actele normative;

32.4. să utilizeze datele de referință privind imaginile faciale și, după caz, să solicite extragerea datelor de bază și a informațiilor suplimentare numai după confirmarea concordanței;

32.5. să utilizeze componenta de schimb automatizat transfrontalier de date numai prin intermediul canalelor și punctelor de contact și potrivit procedurilor stabilite de cadrul normativ;

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

32.7. să nu transmită, să nu divulge și să nu pună la dispoziția terților datele obținute din RIF, cu excepția cazurilor expres prevăzute de actele normative, de tratatele internaționale la care Republica Moldova este parte sau de actele de punere în aplicare a acestora, cu respectarea condițiilor stabilite de autoritatea competentă care a furnizat datele;

32.8. să informeze fără întârziere furnizorul de date sau registratorul competent în cazul în care constată că datele primite sunt inexacte, neactualizate sau au fost transmise cu încălcarea prevederilor legale.

Capitolul IV
ȚINEREA RIF ȘI EFECTUAREA OPERAȚIUNILOR ASUPRA DATELOR DIN RIF

Secțiunea 1
Dispoziții generale privind ținerea RIF

33. RIF se ține în format electronic, prin intermediul SI RIF, în condițiile prevăzute de prezentul Regulament, de actele normative speciale și, după caz, de tratatele internaționale la care Republica Moldova este parte.

34. Ținerea RIF cuprinde ansamblul operațiunilor de recepționare, verificare, introducere, înregistrare, actualizare, rectificare, completare, blocare, radiere, arhivare, consultare, extragere, comparare, validare și furnizare a datelor din RIF, efectuate prin intermediul SI RIF, în limitele competențelor stabilite prin lege și ale profilurilor de acces aprobate.

35. Operațiunile asupra datelor din RIF se efectuează prin intermediul SI RIF numai de către utilizatorii autorizați, în baza rolurilor și profilurilor de acces atribuite, cu respectarea principiilor legalității, necesității, proporționalității, exactității și limitării scopului, precum și a cerințelor privind securitatea informației și trasabilitatea operațiunilor.

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

36.1. componentei naționale a RIF;

36.2. setului de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier de date, constituit și utilizat exclusiv în condițiile prevăzute de actele normative.

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

38. În RIF se introduc și se gestionează, în condițiile prevăzute de actele normative și de prezentul Regulament, înregistrările privind rezultatele comparării automatizate, confirmarea sau infirmarea concordanței, solicitările de căutare automatizată și răspunsurile la acestea, jurnalele operațiunilor și alte

evidențe necesare pentru asigurarea trasabilității și a controlului utilizării datelor din RIF.

39. Orice operațiune asupra datelor din RIF trebuie să fie justificată de scopul legal urmărit, să se întemeieze pe documente, date sau informații provenite din surse autorizate și să se limiteze la datele strict necesare pentru atingerea acestui scop.

Secțiunea a 2-a
Introducerea și înregistrarea datelor în RIF

40. Introducerea datelor în RIF se efectuează prin intermediul SI RIF, de către registratori, în baza documentelor justificative, a datelor furnizate de către autoritățile competente, a informațiilor obținute prin intermediul mecanismelor de interoperabilitate, a rezultatelor activităților de constatare tehnico-științifică sau de expertiză judiciară, precum și a altor surse autorizate de lege.

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

41.1. existența competenței legale pentru efectuarea operațiunii;

41.2. existența temeiului juridic și a documentului justificativ;

41.3. caracterul necesar, relevant și neexcesiv al datelor;

41.4. exactitatea, caracterul complet și actualitatea datelor disponibile;

41.5. calitatea imaginii faciale și conformitatea acesteia cu cerințele necesare pentru prelucrarea ulterioară, inclusiv, după caz, pentru compararea automatizată;

41.6. inexistența unor înregistrări duplicate evidente sau, în cazul identificării acestora, necesitatea aplicării regulilor de consolidare a evidenței.

42. 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 completarea ulterioară a datelor, de îndată ce acestea devin disponibile în condițiile legii.

43. Introducerea unei imagini faciale identificate în RIF se efectuează cu înregistrarea, după caz, a următoarelor date și informații:

43.1. numărul de referință;

43.2. sursa datelor și temeiul juridic al introducerii imaginii faciale;

43.3. autoritatea sau entitatea care a furnizat datele;

43.4. categoria persoanei, potrivit cadrului normativ național în domeniul cooperării polițienești internaționale și actelor normative adoptate în executarea acestuia;

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

43.6. data și ora introducerii;

43.7. datele de identificare ale registratorului care a efectuat operațiunea;

43.8. alte metadate necesare pentru asigurarea trasabilității și a utilizării în conformitate cu prevederile legale.

44. 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.

45. 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 prevăzute de actele normative.

46. Numărul de referință se atribuie la momentul introducerii imaginii în RIF și se utilizează ca identificator unic al obiectului informațional, potrivit structurii stabilite în Conceptul Sistemului informațional „Registrul imaginilor faciale”, inclusiv pentru corelarea acestuia cu datele de bază și cu informațiile suplimentare care pot fi extrase ulterior, în condițiile prevăzute de actele normative.

47. Numărul de referință se utilizează pentru corelarea controlată a imaginii faciale cu metadatele aferente, rezultatele comparării automatizate, înregistrările privind validarea concordanței și, după caz, cu datele de bază și informațiile suplimentare care pot fi extrase ulterior, în condițiile prevăzute de actele normative.

48. 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.

49. Introducerea datelor în setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier de date se efectuează numai pentru categoriile de persoane prevăzute de cadrul normativ național în domeniul cooperării polițienești internaționale și de actele normative adoptate în executarea acestuia și numai dacă sunt îndeplinite condițiile juridice, tehnice și organizatorice aplicabile.

50. Setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier de date se constituie exclusiv 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,

în cazurile, în condițiile și în limitele prevăzute expres de cadrul normativ național în domeniul cooperării polițienești internaționale și, după caz, de actele normative adoptate în executarea acestuia, ale victimelor, cu respectarea principiilor necesității, proporționalității și limitării scopului, precum și a cerințelor privind protecția datelor cu caracter personal.

51. Includerea datelor de referință privind imaginile faciale ale victimelor în setul de date destinat schimbului automatizat transfrontalier de date nu poate avea caracter general sau automat și se efectuează exclusiv în legătură cu un caz individual determinat, în baza unui temei legal expres, cu documentarea necesității, proporționalității, scopului prelucrării și a legăturii dintre datele respective și prevenirea, constatarea sau investigarea infracțiunii. Datele respective se utilizează numai în scopul pentru care au fost incluse în setul de date și cu respectarea cerințelor privind accesul autorizat, jurnalizarea, trasabilitatea și controlul.

52. Datele gestionate în RIF se supun unor regimuri distincte de prelucrare, păstrare, utilizare, furnizare, radiere și arhivare, în funcție de categoria persoanei vizate, de calitatea procesuală sau juridică a acesteia, de scopul prelucrării, de temeiul juridic și de statutul cauzei penale, al dosarului de căutare sau al altei proceduri relevante. Se interzice aplicarea automată a aceluiași regim de prelucrare și păstrare a datelor privind persoanele condamnate, persoanele care au calitatea de bănuit, învinuit sau inculpat, victimele, persoanele dispărute și persoanele reprezentate în imaginile faciale neidentificate.

53. Datele introduse în setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier de date nu pot include date de identificare directă a persoanei și se limitează la datele de referință și la elementele tehnice strict necesare pentru efectuarea căutării automatizate și gestionarea fluxului de schimb. Datele de bază și informațiile suplimentare pot fi extrase și furnizate numai după confirmarea concordanței și în condițiile prevăzute de actele normative.

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

54. Datele din RIF se actualizează fără întârzieri nejustificate în următoarele cazuri:

54.1. intervin modificări privind identitatea sau statutul persoanei;

54.2. sunt recepționate date noi sau rezultate suplimentare ale activităților procedurale, operative, tehnico-științifice sau de expertiză;

54.3. sunt primite date actualizate de la furnizorii de date sau prin intermediul mecanismelor de interoperabilitate;

54.4. necesitatea actualizării rezultă dintr-un act procedural, administrativ sau jurisdicțional;

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

55. Completarea datelor se efectuează atunci când evidența existentă nu conține toate elementele necesare pentru individualizarea obiectului informațional sau a cazului ori pentru stabilirea contextului prelucrării, cu condiția existenței unui temei legal și a unei surse autorizate.

56. Rectificarea datelor din RIF se efectuează în cazul constatării unor inexactități, a caracterului incomplet, neactualizat sau neconform al acestora, din oficiu ori la sesizarea subiecților competenți, inclusiv a furnizorilor de date, a destinatarilor datelor ori a persoanei vizate, în condițiile prevăzute de actele normative.

57. Rectificarea se efectuează cu păstrarea istoricului operațiunilor, astfel încât să poată fi identificate forma anterioară și forma rectificată a datelor, utilizatorul care a efectuat operațiunea, precum și data și temeiul acesteia.

58. Blocarea datelor din RIF se dispune în următoarele cazuri:

58.1. exactitatea datelor este contestată, iar verificarea acestora este în curs de desfășurare;

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

58.3. este necesară conservarea datelor în vederea verificării legalității prelucrării, a efectuării controlului sau a auditului ori a investigației unui incident de securitate;

58.4. restricționarea prelucrării datelor este necesară în alte cazuri prevăzute de actele normative.

59. Pe durata blocării, datele nu pot face obiectul unor noi operațiuni de prelucrare, cu excepția operațiunilor de stocare, protejare, verificare a legalității, exercitare a controlului și a altor operațiuni prevăzute expres de actele normative.

60. În cazul în care datele blocate fac parte și din setul de date de referință destinat schimbului automatizat transfrontalier de date, acestea sunt suspendate sau retrase din componenta respectivă, în măsura necesară pentru prevenirea prelucrării neconforme.

Secțiunea a 4-a
Radierea, arhivarea și păstrarea datelor

61. Radierea datelor din RIF se efectuează în următoarele cazuri:

61.1. s-a constatat lipsa temeiului legal pentru prelucrarea acestora;

61.2. datele au fost introduse în mod eronat sau au fost înregistrate de mai multe ori, iar păstrarea lor separată nu este justificată;

61.3. scopul pentru care datele au fost prelucrate a fost atins, iar păstrarea ulterioară a acestora nu mai are temei legal;

61.4. a expirat termenul de păstrare a datelor;

61.5. radierea este dispusă printr-un act procedural, un act administrativ sau o hotărâre judecătorească ori este necesară în baza unui alt temei prevăzut de lege.

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

63. Înainte de radierea definitivă, datele pot fi arhivate sau păstrate în regim de acces restricționat, în măsura în care acest lucru este necesar pentru îndeplinirea obligațiilor legale privind arhivarea, controlul și auditul, stabilirea răspunderii juridice sau apărarea drepturilor și intereselor legitime.

64. Arhivarea datelor și documentelor aferente RIF se efectuează în conformitate cu legislația în domeniul arhivării, cu nomenclatorul documentelor și cu regulile interne aprobate de către posesor, asigurându-se confidențialitatea, integritatea și accesul restricționat la acestea.

65. Datele gestionate în RIF se păstrează pe perioade determinate sau determinabile, stabilite în mod diferențiat în funcție de categoria obiectului informațional, categoria persoanei vizate, temeiul prelucrării și scopul prelucrării, statutul cauzei penale, al dosarului de căutare sau al altei proceduri relevante, precum și de termenele de păstrare prevăzute de legislația procesual-penală, legislația în domeniul arhivării, actele normative speciale și nomenclatorul documentelor aprobat în condițiile legii.

66. Termenele de păstrare a imaginilor faciale, a datelor de referință, a metadatelor aferente și a înregistrărilor asociate se stabilesc potrivit următoarelor reguli:

66.1. datele referitoare la persoanele care au calitatea de bănuit, învinuit sau inculpat se păstrează pe perioada necesară realizării scopului prelucrării în cadrul cauzei penale sau al procedurii relevante, până la soluționarea definitivă a

cauzei ori finalizarea procedurii respective. În cazul încetării temeiului legal al prelucrării, inclusiv ca urmare a scoaterii persoanei de sub urmărire penală, încetării procesului penal, clasării cauzei sau achitării definitive a persoanei, datele se radiază, se arhivează ori prelucrarea acestora se restricționează, după caz, fără întârzieri nejustificate, cu excepția situațiilor în care păstrarea este impusă de un alt temei legal expres;

66.2. datele referitoare la persoanele condamnate se păstrează pe durata prevăzută de cadrul normativ aplicabil evidenței condamnărilor, executării pedepselor și arhivării cauzelor penale și a documentelor procesuale. După încetarea temeiului legal al păstrării, datele se radiază, se arhivează ori prelucrarea acestora se restricționează, după caz, în condițiile prevăzute de actele normative;

66.3. datele referitoare la victime, în măsura în care prelucrarea acestora este permisă de lege, se păstrează numai pe perioada strict necesară realizării scopului pentru care au fost colectate, inclusiv pentru administrarea probelor, identificarea persoanei, protejarea drepturilor victimei sau exercitarea altor atribuții legale ale autorităților competente;

66.4. imaginile faciale neidentificate se păstrează până la identificarea persoanei sau până la încetarea temeiului legal al păstrării acestora, inclusiv ca urmare a expirării termenului de păstrare aplicabil cauzei penale, dosarului de căutare sau procedurii în legătură cu care au fost introduse în RIF;

66.5. datele referitoare la persoanele dispărute fără veste, la cadavre sau părți ale acestora se păstrează până la identificarea persoanei, încetarea dosarului de căutare sau finalizarea procedurilor legale relevante, după care se radiază, se arhivează ori prelucrarea acestora se restricționează, după caz, în condițiile legii;

66.6. datele de referință incluse în setul destinat schimbului automatizat transfrontalier de date se păstrează numai atât timp cât datele corespunzătoare din componenta națională a RIF sunt valabile, actualizate și îndeplinesc condițiile de includere în setul respectiv. Încetarea temeiului legal al păstrării datelor în componenta națională a RIF determină radierea sau actualizarea corespunzătoare a acestora în setul de date de referință destinat schimbului automatizat transfrontalier de date;

66.7. rezultatele comparării automatizate, lista mostrelor pentru care există posibilitatea unei concordanțe și înregistrările privind confirmarea sau infirmarea concordanței se păstrează pe durata necesară desfășurării cauzei penale, precum și pe perioada necesară efectuării controlului și auditului, verificării legalității prelucrării și stabilirii răspunderii, în condițiile prevăzute de actele normative;

66.8. jurnalele de acces, evidențele operațiunilor și metadatele necesare trasabilității se păstrează pe perioada stabilită prin nomenclatorul documentelor și prin procedurile interne aprobate în condițiile prevăzute de actele normative, dar nu mai puțin decât perioada necesară efectuării auditului și controlului, investigării incidentelor de securitate și verificării legalității prelucrării.

67. Posesorul SI RIF și al RIF asigură revizuirea periodică, cel puțin o dată la 12 luni, a necesității păstrării datelor gestionate în RIF, în special a imaginilor faciale neidentificate, a datelor referitoare la victime și a datelor asociate cauzelor sau procedurilor finalizate.

68. Prelungirea termenului de păstrare a datelor este permisă numai în cazuri justificate de existența unei cauze penale, a unui dosar de căutare, a unei proceduri judiciare, a unei obligații legale de arhivare, a unei proceduri de control sau de audit, de necesitatea investigării unui incident de securitate ori de existența unui alt temei legal expres. Prelungirea se documentează, cu indicarea temeiului legal, a motivelor, a duratei prelungirii și a persoanei sau autorității care a dispus-o.

69. În cazul în care datele din RIF au fost incluse în setul de date de referință destinat schimbului automatizat transfrontalier de date sau au fost furnizate prin intermediul punctului unic de contact ori al punctelor naționale de contact, rectificarea, marcarea, restricționarea prelucrării, radierea sau arhivarea acestora, precum și încetarea temeiului legal al păstrării lor se comunică, fără întârzieri nejustificate, autorității competente responsabile de schimbul de date și informații, în vederea aplicării măsurilor corespunzătoare în privința datelor transmise, potrivit cadrului normativ privind instituirea și funcționarea punctului unic de contact și a punctelor naționale de contact.

70. După expirarea termenelor de păstrare sau după încetarea temeiului legal al prelucrării, datele din RIF se radiază, se arhivează ori se depersonalizează ireversibil, sau, după caz, prelucrarea acestora se restricționează, în condițiile prevăzute de actele normative. Se păstrează exclusiv datele și metadatele necesare pentru efectuarea auditului și controlului, stabilirea răspunderii juridice, raportare statistică sau îndeplinirea obligațiilor legale de arhivare.

71. Radierea, arhivarea, restricționarea prelucrării sau depersonalizarea datelor din RIF se efectuează prin intermediul SI RIF, cu înregistrarea operațiunii, a temeiului legal, a datei efectuării acesteia, a utilizatorului responsabil și, după caz, a documentului sau actului care justifică operațiunea.

Secțiunea a 5-a
Evidența operațiunilor asupra datelor

72. Evidența automată a operațiunilor efectuate asupra datelor din RIF se ține prin intermediul SI RIF și cuprinde operațiunile de introducere, actualizare, rectificare, completare, blocare, radiere, arhivare, consultare, extragere, comparare, validare și transmitere a datelor.

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

73.1. utilizatorul care a efectuat operațiunea;
73.2. rolul utilizatorului și al instituției din care acesta face parte;
73.3. data și ora operațiunii;
73.4. tipul operațiunii efectuate;
73.5. obiectul informațional vizat;
73.6. temeiul legal sau justificarea efectuării operațiunii, după caz;
73.7. sursa datelor sau destinatarul acestora, după caz;
73.8. rezultatul operațiunii.

74. Jurnalele operațiunilor și istoricul modificărilor se păstrează separat, în condiții de securitate, accesul la acestea fiind permis numai persoanelor autorizate, în scopul administrării tehnice, efectuării controlului și auditului, investigării incidentelor de securitate sau verificării legalității prelucrării datelor.

75. Se interzice modificarea, ștergerea sau denaturarea neautorizată a înregistrărilor privind operațiunile efectuate asupra datelor. Încălcarea acestei interdicții atrage răspunderea prevăzută de lege.

76. Regulile tehnice privind formatele de evidență, păstrarea istoricului modificărilor, gestionarea versiunilor, efectuarea copiilor de siguranță și restabilirea datelor se stabilesc de către deținătorul SI RIF, cu aprobarea posesorului SI RIF și al RIF, în conformitate cu prezentul Regulament și cu cerințele în domeniul securității informației și al protecției 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, prin intermediul SI RIF sau al altor canale autorizate prevăzute de actele normative, în limitele competențelor, atribuțiilor funcționale și profilului de acces aprobat.

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

79. Accesul la datele din RIF se acordă exclusiv pentru exercitarea atribuțiilor de serviciu și realizarea scopurilor prevăzute de actele normative și de prezentul Regulament.

80. Accesul la datele din RIF, inclusiv la imaginile faciale, datele de referință privind imaginile faciale, metadatele aferente, informațiile privind rezultatele comparării automatizate și cele privind confirmarea sau infirmarea concordanței, se realizează cu respectarea 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 de date se acordă și se exercită distinct de accesul la componenta națională a RIF, potrivit competențelor stabilite de actele normative și de prezentul Regulament.

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

Secțiunea a 2-a
Categoriile de acces și profilurile de acces

83. În funcție de competențele legale și de necesitățile funcționale, accesul la datele din RIF poate permite, după caz, efectuarea următoarelor 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 actele normative;

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 de către personalul calificat desemnat în acest scop;

83.9. administrarea utilizatorilor, a rolurilor și a profilurilor de acces;

83.10. monitorizarea, controlul și auditul utilizării SI RIF.

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

84.1. funcția deținută;

84.2. atribuțiile legale și de serviciu;

84.3. categoriile de date necesare pentru exercitarea atribuțiilor;
84.4. nivelul de competență operațională sau tehnică;
84.5. necesitatea accesului la datele respective pentru îndeplinirea unei sarcini concrete.

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

86. Fiecărui utilizator i se atribuie un identificator unic de acces, netransmisibil. Se interzice utilizarea datelor de autentificare a unei alte persoane, divulgarea sau transmiterea acestora către alte persoane, precum și permiterea accesului altor persoane prin intermediul propriului cont.

87. Accesul utilizatorilor la datele din RIF și, după caz, la funcționalitățile SI RIF se realizează prin mijloace de autentificare și de control al accesului care respectă cerințele cadrului normativ și ale politicilor de securitate.

88. Dreptul de acces la datele din RIF nu are caracter permanent și se menține numai atât timp cât subzistă temeiul juridic și necesitatea funcțională care au justificat acordarea acestuia.

Secțiunea a 3-a
Acordarea și exercitarea accesului la date

89. Accesul la datele din RIF se acordă în baza unei solicitări motivate a conducătorului autorității sau entității interesate ori a persoanei împuternicite de acesta, cu indicarea temeiului legal, a scopului accesului, a categoriilor de date necesare și a persoanelor pentru care se solicită acordarea profilurilor de acces.

90. Posesorul SI RIF și al RIF, cu participarea deținătorului SI RIF, după caz, examinează solicitarea de acces și decide asupra acordării, limitării sau refuzului accesului, în funcție de următoarele criterii:
90.1. existența competenței legale;
90.2. compatibilitatea scopului declarat cu scopurile RIF;
90.3. necesitatea și proporționalitatea accesului solicitat;
90.4. existența măsurilor tehnice și organizatorice necesare pentru utilizarea legală și în condiții de securitate a datelor.

91. Acordarea accesului se refuză în cazul în care nu este demonstrată existența competenței legale, nu este justificată necesitatea funcțională a accesului sau nu sunt întrunite condițiile de securitate și de conformitate.

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

93. Utilizatorii autorizați pot accesa datele din RIF numai în legătură cu îndeplinirea unei sarcini concrete de serviciu, desfășurarea unei proceduri legale determinate sau, după caz, examinarea unui caz individual documentat.

94. Se interzice accesarea datelor în scopul verificării generale sau exploratorii, al realizării unor analize statistice individualizate neautorizate ori în alte scopuri incompatibile cu temeiul legal al prelucrării.

95. În cazul accesului la datele necesare cooperării polițienești internaționale, inclusiv la setul de date de referință destinat schimbului automatizat transfrontalier de date, utilizatorii acționează numai prin intermediul punctelor de contact și al canalelor securizate, cu respectarea procedurilor prevăzute de cadrul normativ național în domeniul cooperării polițienești internaționale, de tratatele internaționale la care Republica Moldova este parte și de actele de punere în aplicare a acestora.

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

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

96.1. acces direct și autorizat la interfețele SI RIF, în conformitate cu profilul de acces;

96.2. extrase, rapoarte sau alte documente de ieșire generate prin intermediul SI RIF;

96.3. schimb automatizat transfrontalier de date prin intermediul mecanismelor de interoperabilitate, în condițiile prevăzute de actele normative;

96.4. alte modalități prevăzute expres de cadrul normativ.

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

98. Datele din RIF se furnizează în volumul minim necesar realizării scopului pentru care au fost solicitate.

99. Datele de identificare directă a persoanei și alte informații suplimentare asociate unei imagini faciale pot fi furnizate numai în condițiile

prevăzute de actele normative, după caz, în urma confirmării concordanței, și subiecților care au competența legală de a primi aceste date.

100. Datele primite din RIF nu pot fi transmise ulterior altor autorități, instituții, entități sau persoane decât în cazurile prevăzute expres de lege ori cu autorizarea prealabilă a autorității furnizoare, atunci când cadrul normativ impune o astfel de condiție.

101. În cadrul schimbului automatizat transfrontalier de date, utilizarea și furnizarea ulterioară a datelor se realizează cu respectarea restricțiilor, condițiilor și limitărilor comunicate de către autoritatea furnizoare, precum și a prevederilor cadrului normativ în domeniul cooperării polițienești internaționale.

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

102. Datele din RIF se utilizează exclusiv în următoarele scopuri:

102.1. prevenirea, constatarea și investigarea infracțiunilor;

102.2. identificarea sau verificarea identității persoanelor, în condițiile prevăzute de actele normative;

102.3. căutarea persoanelor dispărute;

102.4. identificarea cadavrelor sau a părților acestora;

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

102.6. realizarea schimbului automatizat transfrontalier de date de referință privind imaginile faciale, în condițiile prevăzute de actele normative;

102.7. realizarea altor scopuri expres prevăzute de actele normative și compatibile cu destinația RIF.

103. Se interzice utilizarea datelor din RIF în alte scopuri decât cele prevăzute în prezenta secțiune și de cadrul normativ.

104. Se interzice utilizarea datelor din RIF:

104.1. pentru supravegherea generalizată nediferențiată;

104.2. pentru efectuarea unor interogări exploratorii sau nedeterminate;

104.3. pentru crearea unor profiluri discriminatorii;

104.4. pentru adoptarea unor decizii care produc efecte juridice sau afectează semnificativ persoana vizată, exclusiv pe baza unui rezultat automatizat nevalidat, în cazurile în care legea impune verificarea de către o persoană;

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

105. Utilizatorii și destinatarii datelor din RIF au următoarele obligații:

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

105.2. să asigure 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 SI RIF și al RIF sau deținătorul SI RIF cu privire la orice acces neautorizat, incident de securitate, eroare sau neconcordanță constatată;

105.5. să nu modifice, să nu copieze, să nu exporte, să nu distribuie sau să nu stocheze datele cu încălcarea condițiilor prevăzute de actele normative și a limitelor profilului de acces acordat.

106. Persoana vizată își poate exercita drepturile la informare, acces, rectificarea și completarea datelor, la restricționarea prelucrării, la opoziția și la ștergerea datelor, precum și dreptul de contestare, în condițiile și limitele prevăzute de legislația privind protecția datelor cu caracter personal și de actele normative 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 sau modificarea atribuțiilor de serviciu ale persoanei;

107.2. încetarea temeiului legal sau a necesității funcționale care au justificat acordarea accesului;

107.3. constatarea utilizării neconforme sau abuzive a datelor;

107.4. nerespectarea obligațiilor de confidențialitate și de securitate;

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

107.6. alte cazuri prevăzute de actele normative sau de actele administrative interne adoptate în temeiul acestora.

108. Suspendarea sau revocarea accesului nu exonerează persoana de răspunderea pentru operațiunile efectuate anterior și nu o scutește de obligația de a păstra confidențialitatea datelor la care a avut acces.

109. Acordarea, modificarea, suspendarea sau revocarea drepturilor de acces la datele din RIF se înregistrează în SI RIF și se consemnează în documentele interne privind administrarea utilizatorilor și a 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 gestionate în RIF reprezintă operațiunea tehnică realizată prin intermediul SI RIF, prin care imaginea facială supusă verificării este comparată cu datele comparative disponibile, în vederea identificării unei posibile concordanțe.

111. Compararea automatizată se efectuează exclusiv în scopurile prevăzute de actele normative, în limitele competențelor autorității solicitante și cu respectarea principiilor legalității, necesității, proporționalității, limitării scopului, minimizării datelor, trasabilității și securității informației.

112. Compararea automatizată a imaginilor faciale gestionate în RIF poate fi efectuată:

112.1. prin compararea cu datele gestionate în componenta națională a RIF;

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

112.3. prin corelarea controlată cu date și metadate relevante din sistemele și resursele informaționale interoperabile, prin intermediul SI RIF, în măsura permisă de lege.

113. Compararea automatizată se efectuează exclusiv în legătură cu un caz individual determinat și documentat. Se interzice inițierea unor interogări generale, exploratorii sau preventive fără un scop determinat, precum și a unor interogări în alte scopuri incompatibile cu cadrul normativ.

114. Compararea automatizată a imaginilor faciale nu poate produce, prin ea însăși, efecte operaționale definitive în lipsa validării umane a concordanței de către personalul calificat, în cazurile în care cadrul normativ național în domeniul cooperării polițienești internaționale, actele de punere în aplicare a acestuia sau prezentul Regulament impun o asemenea verificare.

Secțiunea a 2-a
Inițierea comparării automatizate

115. Compararea automatizată a imaginilor faciale gestionate în RIF se inițiază prin intermediul SI RIF, de către utilizatorii autorizați, în limitele rolului și profilului de acces atribuite, în baza unui temei legal și a unei necesități funcționale concrete.

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

116.1. autoritatea sau entitatea solicitantă;

116.2. utilizatorul care inițiază operațiunea;

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

116.4. imaginea facială supusă comparării;

116.5. temeiul legal și scopul operațiunii;

116.6. data și ora inițierii;

116.7. alte metadate necesare pentru urmărirea fluxului operațional.

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

117.1. dacă imaginea facială are o calitate suficientă pentru efectuarea comparării;

117.2. existența temeiului legal și a cazului individual care justifică efectuarea comparării;

117.3. încadrarea solicitării în limitele competenței sale;

117.4. dacă datele utilizate sunt necesare și relevante pentru atingerea scopului urmărit;

117.5. dacă solicitarea nu constituie o interogare cu caracter exploratoriu sau discriminatoriu.

118. Imaginile faciale neidentificate gestionate în RIF pot fi supuse comparării automatizate prin intermediul SI RIF, cu păstrarea marcării distincte a acestora pe întreaga durată a prelucrării, până la eventuala identificare ulterioară a persoanei, în condițiile prevăzute de actele normative.

119. În cadrul mecanismului de căutare automatizată transfrontalieră, solicitarea se formulează și se transmite numai prin canalele și punctele de contact, precum și potrivit procedurilor stabilite de cadrul normativ național în domeniul cooperării polițienești internaționale și de actele de punere în aplicare a acestuia.

Secțiunea a 3-a
Efectuarea comparării automatizate și formarea rezultatului

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

121. În procesul comparării automatizate, prin intermediul SI RIF se efectuează, după caz:

121.1. compararea 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 indica, după caz:

122.1. absența unei concordanțe;

122.2. existența unei posibile concordanțe;

122.3. existența mai multor concordanțe posibile;

122.4. imposibilitatea tehnică de a obține un rezultat concludent.

123. Rezultatul comparării automatizate se înregistrează în RIF, prin intermediul SI RIF, cu indicarea cel puțin a următoarelor date:

123.1. identificatorul rezultatului comparării;

123.2. numărul de referință al imaginii faciale supuse comparării;

123.3. numărul de referință al mostrei comparative sau numerele de referință ale mostrelor comparative relevante, după caz;

123.4. data și ora efectuării comparării;

123.5. tipul și statutul rezultatului;

123.6. gradul de asemănare, după caz;

123.7. componenta tehnică prin intermediul căreia a fost generat rezultatul;

123.8. utilizatorul sau procesul 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 exclusiv datele strict necesare

pentru identificarea solicitării, urmărirea fluxului de schimb de date și gestionarea concordanței, fără a permite identificarea directă a persoanei, în condițiile prevăzute de actele normative.

126. Operațiunile de transmitere a solicitărilor, de recepționare a răspunsurilor, de gestionare a rezultatelor, de formare a listei mostrelor pentru care există posibilitatea unei concordanțe, de validare a concordanței, de jurnalizare, de auditare și de asigurare a trasabilității în cadrul componentei de schimb automatizat transfrontalier de date se efectuează în conformitate cu prevederile prezentului Regulament și cu documentația tehnică a SI RIF, cu respectarea cadrului normativ.

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

127. Lista mostrelor pentru care există posibilitatea unei concordanțe reprezintă un rezultat tehnic intermediar al comparării automatizate, generat prin intermediul SI RIF și constituit din una sau mai multe mostre comparative, pe baza nivelului de asemănare determinat potrivit regulilor de procesare aplicabile.

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

129. Lista mostrelor pentru care există posibilitatea unei concordanțe se formează exclusiv pentru un caz individual, în condițiile prevăzute de actele normative, și include mostre comparative selectate automat prin intermediul SI RIF, în ordinea descrescătoare a nivelului de asemănare. Numărul maxim de mostre incluse în listă, precum și pragurile tehnice pentru generarea acesteia, se stabilesc în documentația tehnică a SI RIF, aprobată în condițiile prevăzute de actele normative.

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

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

131.1. nu se extrag și nu se furnizează date care permit identificarea directă a persoanei;

131.2. nu se furnizează informații suplimentare din sistemele-sursă interoperabile, cu excepția celor strict necesare pentru validarea concordanței, în condițiile prevăzute de actele normative;

131.3. nu se dispune nicio măsură procesuală, operativă sau administrativă și nu se fundamentează nicio astfel de măsură exclusiv pe baza listei respective.

132. Lista mostrelor pentru care există posibilitatea unei concordanțe nu poate constitui temei pentru dispunerea unor măsuri procesuale, speciale de investigație sau administrative, inclusiv a celor privative sau restrictive de drepturi, ori a altor măsuri similare. Asemenea măsuri pot fi dispuse numai în condițiile legii, în baza temeiurilor juridice și probatorii, după validarea concordanței și, după caz, coroborarea acesteia cu alte date, informații sau probe relevante.

133. Validarea concordanței se efectuează prin examinarea manuală a rezultatului comparării automatizate și, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe, cu consemnarea obligatorie în RIF, prin intermediul SI RIF, a următoarelor date:

133.1. identitatea sau identificatorul utilizatorului care a efectuat validarea;

133.2. data și ora validării;

133.3. mostra sau mostrele examinate;

133.4. rezultatul validării – confirmarea, infirmarea sau caracterul neconcludent al concordanței;

133.5. observațiile relevante care au stat la baza validării, după caz.

134. În cazul infirmării concordanței, lista mostrelor pentru care există posibilitatea unei concordanțe își păstrează statutul de rezultat tehnic intermediar și poate fi utilizată exclusiv în scopul jurnalizării, controlului, auditului, verificării ulterioare a legalității prelucrării și îmbunătățirii funcționării SI RIF, în condițiile prevăzute de actele normative.

135. În cazul confirmării concordanței, extragerea și furnizarea datelor de bază și a informațiilor suplimentare se efectuează numai în condițiile prevăzute de prezentul Regulament, de legea specială privind cooperarea polițienească internațională și de celelalte acte normative aplicabile.

Secțiunea a 5-a
Validarea concordanței

136. Validarea concordanței reprezintă verificarea de către personalul calificat a rezultatului comparării automatizate și, după caz, a listei mostrelor pentru care există posibilitatea unei concordanțe, în vederea confirmării sau infirmării concordanței ori a constatării caracterului neconcludent al rezultatului.

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

138. Persoana care a participat, în calitate de personal calificat, la validarea concordanței rezultate în urma comparării automatizate efectuate prin intermediul SI RIF nu poate participa ulterior, în aceeași cauză, în calitate de specialist sau expert judiciar, la examinarea, verificarea ori evaluarea aceluiași rezultat sau a aceleiași concordanțe.

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

139.1. identificarea unei persoane sau verificarea identității acesteia;

139.2. individualizarea unui caz;

139.3. extragerea datelor de bază sau a informațiilor suplimentare;

139.4. furnizarea datelor în cadrul cooperării polițienești internaționale;

139.5. dispunerea unei măsuri operaționale sau procedurale care poate produce efecte juridice ori consecințe de fapt relevante.

140. În procesul de validare a concordanței, personalul calificat examinează cel puțin următoarele elemente:

140.1. imaginea facială supusă comparării;

140.2. mostra sau mostrele comparative indicate prin intermediul SI RIF;

140.3. nivelul de asemănare și relevanța rezultatului tehnic;

140.4. calitatea imaginilor comparate;

140.5. contextul cazului individual;

140.6. existența unor elemente care pot genera confuzii, erori sau concluzii eronate.

141. În urma validării, rezultatul se consemnează după cum urmează:

141.1. concordanță confirmată;

141.2. concordanță infirmată;

141.3. rezultat neconcludent, în cazul în care datele disponibile nu permit formularea unei concluzii suficient de certe și sunt necesare verificări suplimentare.

142. În cazul în care autoritatea competentă a Republicii Moldova are calitatea de autoritate solicitată în cadrul schimbului automatizat transfrontalier de date, confirmarea concordanței se efectuează numai după examinarea manuală a rezultatului comparării automatizate și, după caz, a listei mostrelor pentru care

există posibilitatea unei concordanțe de către cel puțin un membru al personalului calificat, în condițiile prevăzute de actele normative.

143. 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 prevăzute de lege.

144. În situația infirmării concordanței, rezultatul comparării nu poate constitui temei pentru extragerea sau furnizarea datelor de bază și a informațiilor suplimentare, acesta putând fi păstrat în RIF, prin intermediul SI RIF, exclusiv în scopul asigurării trasabilității, controlului și auditului.

Secțiunea a 6-a
Evidența rezultatelor comparării și a validării

145. În RIF se ține, prin intermediul SI RIF, evidența distinctă a următoarelor:

145.1. solicitările de comparare automatizată;

145.2. rezultatele comparării automatizate;

145.3. validările efectuate;

145.4. confirmările sau infirmările concordanței;

145.5. operațiunile ulterioare efectuate în legătură cu rezultatele comparării și ale validării.

146. Înregistrarea privind confirmarea sau infirmarea concordanței conține cel puțin următoarele date:

146.1. identificatorul validării;

146.2. identificatorul rezultatului comparării;

146.3. data și ora validării;

146.4. rezultatul validării;

146.5. datele de identificare ale persoanei calificate care a efectuat validarea;

146.6. observațiile relevante care justifică confirmarea sau infirmarea concordanței, după caz;

146.7. datele de referință care permit stabilirea legăturii cu cazul individual și cu eventualele operațiuni ulterioare.

147. Toate rezultatele comparării și ale validării se păstrează în RIF, prin intermediul SI RIF, cu asigurarea istoricului operațiunilor, a trasabilității complete și a posibilității verificării ulterioare în scopul efectuării controlului și auditului, investigării incidentelor de securitate sau verificării legalității prelucrării.

148. Rezultatele comparării automatizate și ale validării concordanței pot fi utilizate pentru extragerea datelor de bază și a informațiilor suplimentare numai în cazul în care concordanța a fost confirmată și în condițiile prevăzute de prezentul Regulament și de actele normative aplicabile.

149. În cazul confirmării unei concordanțe în cadrul mecanismului de schimb automatizat transfrontalier de date, furnizarea ulterioară a datelor de bază și a informațiilor suplimentare se efectuează prin canalele și punctele de contact, precum și potrivit procedurilor stabilite de cadrul normativ național în domeniul cooperării polițienești internaționale și de actele de punere în aplicare a acestuia.

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

Capitolul VII
INTEROPERABILITATEA ȘI SCHIMBUL DE DATE

Secțiunea 1
Dispoziții generale

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

152. Interoperabilitatea SI RIF se asigură, după caz:

152.1. la nivel național, prin schimbul de date cu sistemele și resursele informaționale de stat relevante;

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

153. În cadrul schimbului de date se transmit numai datele strict necesare și relevante pentru scopul urmărit, cu respectarea regimului juridic aplicabil fiecărei categorii de date și a restricțiilor stabilite de cadrul normativ național în

domeniul cooperării polițienești internaționale, de actele de punere în aplicare a acestuia sau de autoritatea furnizoare, după caz.

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

Secțiunea a 2-a
Interoperabilitatea la nivel național

155. În cazul în care, pentru introducerea, actualizarea, rectificarea, completarea, blocarea, radierea sau utilizarea datelor în RIF, legislația prevede deținerea unor date sau documente disponibile în resursele informaționale ale altor autorități sau entități publice, acestea se preiau sau se furnizează prin intermediul platformei guvernamentale de interoperabilitate (MConnect), în condițiile prevăzute de actele normative.

156. Pentru publicarea și consumul evenimentelor de sistem relevante pentru interoperabilitate, SI RIF poate utiliza componenta MConnect Events, prin intermediul interfețelor de programare a aplicațiilor (API), cu respectarea cadrului normativ, a ghidului tehnic publicat de Instituția publică „Agenția de Guvernare Electronică”, a cerințelor de securitate, a acordurilor sau contractelor privind schimbul de date și a documentației tehnice aferente SI RIF.

157. Evenimentele de sistem expuse prin MConnect Events se stabilesc în documentația tehnică aferentă SI RIF și se limitează la cele necesare pentru asigurarea interoperabilității, cu respectarea regimului juridic al datelor, a principiului necesității și proporționalității, precum și a cerințelor privind protecția datelor cu caracter personal, securitatea cibernetică, jurnalizarea și trasabilitatea.

158. Interoperabilitatea la nivel național se realizează numai cu sistemele și resursele informaționale relevante pentru scopurile RIF, fără a înlocui funcțiile de evidență primară ale acestora și fără a afecta regimul juridic al datelor gestionate în cadrul lor.

159. În cadrul interoperabilității la nivel național, SI RIF poate prelua sau furniza, după caz, următoarele categorii de date și documente:

159.1. date de identificare necesare pentru verificarea identității persoanei;

159.2. date și documente necesare pentru individualizarea cazului;

159.3. date necesare pentru actualizarea și rectificarea înregistrărilor;

159.4. date necesare pentru verificarea calității și coerenței evidențelor;

159.5. alte date prevăzute de actele normative, în măsura în care acestea sunt necesare pentru exercitarea atribuțiilor autorităților competente.

160. Schimbul de date prin intermediul interoperabilității la nivel național se efectuează pe baza serviciilor de platformă, a interfețelor tehnice, a regulilor de validare, a nomenclatoarelor și a specificațiilor aprobate potrivit cadrului normativ.

161. Subiecții care participă la formarea și actualizarea RIF prin preluarea sau furnizarea datelor în cadrul interoperabilității sunt autoritățile și entitățile publice care dețin, administrează sau gestionează sisteme și resurse informaționale relevante, în limitele competențelor prevăzute de actele normative

162. În cazul în care, prin intermediul interoperabilității, sunt recepționate date care indică existența unor neconcordanțe sau erori ori necesitatea efectuării unor verificări suplimentare, datele respective se supun procedurilor interne de verificare, rectificare sau actualizare prevăzute de prezentul Regulament.

Secțiunea a 3-a
Furnizarea și preluarea datelor la nivel național

163. Furnizarea datelor din RIF către autoritățile și entitățile publice la nivel național se efectuează numai dacă acestea sunt abilitate prin lege să primească asemenea date și numai în măsura necesară exercitării atribuțiilor lor.

164. Datele din RIF pot fi puse la dispoziția subiecților autorizați la nivel național prin următoarele modalități:

164.1. prin intermediul platformei guvernamentale de interoperabilitate (MConnect);

164.2. prin acces direct autorizat la interfețele SI RIF, în limitele profilului de acces atribuit;

164.3. prin extrase, rapoarte sau alte documente generate de sistem, în condițiile prevăzute de actele normative;

164.4. prin alte modalități prevăzute expres de cadrul normativ.

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

165.1. se furnizează numai datele strict necesare pentru realizarea scopului declarat;

165.2. se aplică, după caz, măsuri de restricționare a accesului la date, de pseudonimizare sau de limitare a volumului de date furnizate;

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

165.4. se asigură trasabilitatea fiecărei operațiuni de furnizare și preluare a datelor, precum și posibilitatea verificării ulterioare a acesteia.

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

166. SI RIF contribuie, în condițiile prevăzute de actele normative, de tratatele internaționale și de actele de punere în aplicare a acestora, la realizarea schimbului automatizat transfrontalier al datelor de referință privind imaginile faciale, precum și la interacțiunea cu infrastructurile și mecanismele externe utilizate în cadrul cooperării polițienești internaționale.

167. Funcționalitățile aferente schimbului automatizat transfrontalier al datelor de referință privind imaginile faciale se pun în aplicare numai după îndeplinirea condițiilor juridice, organizatorice și tehnice necesare, inclusiv, după caz, după efectuarea notificărilor și desemnărilor necesare și adoptarea actelor normative de punere în aplicare a cadrului normativ național în domeniul cooperării polițienești internaționale.

168. Schimbul automatizat transfrontalier al datelor de referință privind imaginile faciale se realizează exclusiv în cazuri individuale, prin intermediul autorității naționale competente și/sau al punctelor de contact competente, utilizând canalele, infrastructurile și mecanismele stabilite de cadrul normativ național în domeniul cooperării polițienești internaționale, de tratatele internaționale la care Republica Moldova este parte și de actele de punere în aplicare a acestora.

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

170. 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 sau retragere a acestor date sunt stabilite de cadrul normativ național în domeniul cooperării polițienești internaționale și de actele de punere în aplicare a acestuia.

171. Transmiterea și recepționarea datelor de referință privind imaginile faciale în cadrul schimbului automatizat transfrontalier de date se efectuează cu asigurarea confidențialității, integrității și autenticității acestora, inclusiv prin

utilizarea criptării și a altor măsuri tehnice și organizatorice adecvate, în condițiile legii.

172. SI RIF asigură separarea funcțională și logică a componentei naționale de setul de date de referință destinat schimbului automatizat transfrontalier de date, precum și aplicarea unor profiluri de acces și a unor fluxuri de utilizare distincte pentru fiecare dintre acestea.

Secțiunea a 5-a
Furnizarea datelor de bază și a informațiilor suplimentare după confirmarea concordanței

173. După confirmarea concordanței, SI RIF poate fi utilizat pentru extragerea și furnizarea datelor de bază și a informațiilor suplimentare aferente numărului de referință identificat, în condițiile prevăzute de actele normative.

174. Furnizarea datelor de bază și a informațiilor suplimentare după confirmarea concordanței se efectuează numai cu respectarea următoarelor condiții:

174.1. datele și informațiile se furnizează exclusiv subiecților autorizați prin lege;

174.2. furnizarea se efectuează prin canalele și procedurile prevăzute pentru cooperarea polițienească internațională;

174.3. datele și informațiile solicitate sunt necesare și proporționale în raport cu scopul urmărit;

174.4. se respectă restricțiile și condițiile stabilite de lege ori, după caz, de autoritatea furnizoare.

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

176. 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, în condițiile prevăzute de legea specială în domeniul cooperării polițienești internaționale.

177. În cazul în care Republica Moldova are calitatea de stat solicitant, datele de bază și informațiile suplimentare primite în urma confirmării concordanței pot fi utilizate numai în scopul pentru care au fost solicitate și în

limitele stabilite de cadrul normativ și de eventualele condiții comunicate de către autoritatea furnizoare.

Secțiunea a 6-a
Restricții și evidența schimbului de date

178. Se interzice utilizarea mecanismelor de interoperabilitate și de schimb de date:

178.1. în lipsa unui temei legal;

178.2. în afara competențelor atribuite;

178.3. în scopuri generale, exploratorii ori discriminatorii;

178.4. pentru eludarea regimului juridic al accesului la date;

178.5. pentru transmiterea unor date excesive sau nerelevante.

179. Orice operațiune de consum, furnizare, transmitere sau recepționare a datelor prin intermediul interoperabilității ori în cadrul schimbului automatizat transfrontalier de date se înregistrează în evidențele SI RIF, astfel încât să se asigure identificarea utilizatorului sau a procesului tehnic care a efectuat operațiunea, a datei și orei efectuării acesteia, a temeiului juridic al operațiunii, a categoriei de date schimbate și a destinatarului sau a sursei acestora, după caz.

180. Evidențele privind schimbul de date se păstrează în condiții de securitate și pot fi utilizate în scopul efectuării controlului și auditului, verificării legalității prelucrării datelor, investigării incidentelor de securitate și stabilirii răspunderii, în condițiile legii.

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

Capitolul VIII
SECURITATEA, JURNALIZAREA, MONITORIZAREA, CONTROLUL ȘI AUDITUL

Secțiunea 1
Dispoziții generale

182. Securitatea, jurnalizarea, monitorizarea, controlul și auditul în cadrul RIF se asigură în scopul garantării legalității prelucrării datelor, al protejării confidențialității, integrității, disponibilității și autenticității datelor, al asigurării rezilienței SI RIF, al prevenirii accesului neautorizat, al detectării utilizărilor

neconforme și al asigurării trasabilității complete a operațiunilor efectuate în sistem.

183. Măsurile de securitate, jurnalizare, monitorizare, control și audit prevăzute în prezentul capitol se aplică întregului ciclu de viață al datelor gestionate prin intermediul SI RIF, inclusiv în cadrul operațiunilor de colectare, recepționare, introducere, stocare, actualizare, rectificare, blocare, radiere, arhivare, comparare automatizată, validare a concordanței, interoperabilitate și schimb de date.

184. Posesorul, deținătorul, 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 prin prezentul Regulament, prin actele administrative aprobate în temeiul acestuia și prin legislația în domeniul protecției datelor cu caracter personal și al securității cibernetice.

185. Posesorul aprobă procedurile interne privind securitatea, administrarea accesului, jurnalizarea, monitorizarea și auditul SI RIF, iar deținătorul asigură implementarea tehnică a acestora.

186. Înainte de punerea în exploatare a SI RIF, de operaționalizarea componentei de schimb automatizat transfrontalier de date, precum și de implementarea unor modificări semnificative ale sistemului care pot genera riscuri ridicate pentru drepturile și libertățile persoanelor vizate, posesorul asigură efectuarea evaluării impactului asupra protecției datelor cu caracter personal, în condițiile Legii nr. 195/2024 privind protecția datelor cu caracter personal, precum și implementarea măsurilor tehnice și organizatorice necesare pentru diminuarea riscurilor identificate.

Secțiunea a 2-a
Măsurile de securitate ale SI RIF

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

187.1. autentificarea utilizatorilor;
187.2. autorizarea și controlul accesului;
187.3. asigurarea confidențialității datelor;
187.4. asigurarea integrității și exactității datelor;
187.5. asigurarea disponibilității și continuității funcționării acestuia;
187.6. asigurarea autenticității și trasabilității operațiunilor;
187.7. prevenirea, detectarea și limitarea incidentelor de securitate;

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

188. Mecanismele tehnice de securitate, autentificare, autorizare, criptare, jurnalizare, trasabilitate, monitorizare, asigurare a disponibilității și continuității funcționării, precum și de recuperare, aferente SI RIF, inclusiv componentei de schimb automatizat transfrontalier de date, se stabilesc în documentația tehnică a SI RIF și în politicile de securitate aprobate, cu respectarea cadrului normativ și a standardelor europene și internaționale relevante.

189. Accesul la funcționalitățile SI RIF se efectuează numai prin mecanisme de autentificare și control al accesului conforme cu cadrul normativ și cu politicile de securitate aprobate, inclusiv, după caz, prin utilizarea serviciilor guvernamentale comune de autentificare.

190. Datele gestionate prin intermediul SI RIF se protejează împotriva accesării, copierii, modificării, distrugerii, divulgării, transmiterii sau utilizării neautorizate, inclusiv prin aplicarea unor măsuri de segmentare logică, separare a rolurilor, restricționare a privilegiilor, criptare, protecție a comunicațiilor și a altor măsuri tehnice adecvate.

191. Componenta națională a RIF și setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier de date se protejează distinct, prin aplicarea unor măsuri diferențiate de acces, utilizare, transmitere și administrare, în conformitate cu regimul juridic aplicabil fiecăreia dintre acestea.

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

193. În cazul apariției unei amenințări cibernetice, al producerii unui incident de securitate, al constatării unei neconformități grave sau al existenței unui risc iminent pentru legalitatea ori securitatea 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 aplicarea măsurilor necesare pentru remedierea situației.

Secțiunea a 3-a
Jurnalizarea operațiunilor

194. 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, precum și de administrare a conturilor sau a profilurilor de acces.

195. Jurnalizarea trebuie să permită identificarea cel puțin a următoarelor elemente:

195.1. utilizatorului sau procesului tehnic care a efectuat operațiunea;

195.2. rolului și instituției de apartenență, după caz;

195.3. datei și orei operațiunii;

195.4. tipului operațiunii efectuate;

195.5. obiectului informațional vizat;

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

195.7. sursei sau destinatarului datelor, după caz;

195.8. rezultatului operațiunii.

196. Evidențele de jurnalizare se păstrează în condiții de securitate, separat de mediile operaționale, cu asigurarea protecției împotriva modificării, ștergerii, divulgării sau accesării neautorizate.

197. 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.

198. Accesul la jurnalele SI RIF este permis numai persoanelor autorizate în mod expres în scopul administrării tehnice, asigurării securității, efectuării controlului intern și auditului, investigării incidentelor, verificării legalității prelucrării datelor sau stabilirii răspunderii, în condițiile prevăzute de actele normative.

199. Modificarea, alterarea, ștergerea ori ascunderea neautorizată a înregistrărilor din jurnalele SI RIF este interzisă și atrage răspunderea în condițiile legii.

Secțiunea a 4-a
Monitorizarea accesării și utilizării datelor din RIF

200. Monitorizarea accesării și utilizării datelor din RIF reprezintă activitatea continuă de supraveghere a funcționării tehnice a SI RIF, a utilizării datelor din RIF în scopuri operaționale și a respectării cerințelor de securitate și legalitate în procesul de prelucrare a acestora.

201. Monitorizarea accesării și utilizării datelor din RIF are următoarele obiective:

201.1. verificarea funcționalității continue a sistemului;

201.2. identificarea accesărilor neautorizate sau neobișnuite;

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

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

201.5. examinarea periodică a jurnalelor de sistem și a operațiunilor de prelucrare a datelor;

201.6. evaluarea necesității aplicării măsurilor de remediere, de restricționare sau de suspendare a accesului.

202. Posesorul SI RIF și al RIF monitorizează ținerea RIF și utilizarea datelor din acesta, inclusiv în cadrul componentei de schimb automatizat transfrontalier de date, iar deținătorul SI RIF asigură monitorizarea tehnică permanentă a funcționalității sistemului și informează posesorul cu privire la incidentele, deficiențele și riscurile identificate.

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

Secțiunea a 5-a
Controlul intern și auditul

204. Controlul intern privind accesarea, utilizarea și prelucrarea datelor din RIF, inclusiv operațiunile efectuate prin intermediul SI RIF, se exercită de către posesorul SI RIF și al RIF și, după caz, de către alte structuri competente, în limitele atribuțiilor stabilite prin lege și prin actele administrative interne.

205. Controlul intern vizează, după caz:

205.1. legalitatea accesării, utilizării și prelucrării datelor din RIF;

205.2. respectarea profilurilor de acces și a separării rolurilor în cadrul SI RIF;

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

205.4. respectarea cerințelor privind securitatea, confidențialitatea, integritatea și trasabilitatea datelor din RIF;

205.5. respectarea obligațiilor de jurnalizare și de păstrare a evidențelor operațiunilor efectuate asupra datelor din RIF prin intermediul SI RIF;

205.6. conformitatea operațiunilor de accesare, utilizare și prelucrare a datelor din RIF cu prevederile prezentului Regulament și ale actelor administrative interne aprobate în temeiul acestuia.

206. În cazul unei încălcări a securității datelor cu caracter personal, operatorul notifică Centrul Național pentru Protecția Datelor cu Caracter Personal, în condițiile prevăzute la art. 33 alin. (1) din Legea nr. 195/2024 privind protecția datelor cu caracter personal, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care aceasta este puțin susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea nu se efectuează în termen de 72 de ore, aceasta este însoțită de o explicație motivată a întârzierii.

207. Deținătorul, registratorii, furnizorii, destinatarii și utilizatorii SI RIF informează fără întârziere posesorul cu privire la orice incident de securitate, vulnerabilitate, acces neautorizat, divulgare neautorizată, pierdere, modificare, distrugere, indisponibilitate sau prelucrare neconformă a datelor din RIF de care au luat cunoștință și acordă sprijinul necesar pentru documentarea, evaluarea, notificarea și remedierea incidentului.

208. Auditul se efectuează periodic sau ori de câte ori este necesar, în scopul evaluării conformității juridice, organizatorice și tehnice a operațiunilor de accesare, utilizare și prelucrare a datelor din RIF, inclusiv a celor efectuate prin intermediul SI RIF, al verificării eficacității măsurilor de securitate și trasabilitate, precum și al identificării riscurilor și vulnerabilităților.

209. Auditul poate avea, după caz, caracter tehnic, de securitate, de conformitate, de protecție a datelor cu caracter personal sau mixt, în funcție de obiectul auditului și de necesitatea de verificare.

210. În cadrul auditului, auditorii sau persoanele împuternicite pot avea acces, în limitele competențelor legale, la jurnalele SI RIF, evidențele operațiunilor efectuate asupra datelor din RIF, registrele de acces, documentele

justificative, procedurile interne, rapoartele privind incidentele de securitate, configurațiile tehnice relevante și alte materiale necesare pentru verificarea legalității, securității, trasabilității și conformității prelucrării datelor.

211. Rezultatele controlului intern și ale auditului se consemnează în acte de constatare, rapoarte sau alte documente interne, care cuprind, după caz, neconformitățile identificate, riscurile constatate, măsurile de remediere recomandate, termenele de executare a acestora și subiecții responsabili de executare.

212. Posesorul SI RIF și al RIF dispune măsurile de remediere necesare în baza constatărilor rezultate în urma controlului intern sau a auditului și monitorizează executarea acestora.

Secțiunea a 6-a
Gestionarea incidentelor și răspunderea

213. Orice utilizator, registrator, furnizor de date, destinatar al datelor sau alt subiect care constată un incident de securitate, un acces neautorizat, o pierdere de date, o neconcordanță relevantă sau o utilizare neconformă a SI RIF este obligat să informeze fără întârziere deținătorul și posesorul, potrivit procedurilor interne.

214. Gestionarea incidentelor de securitate include, după caz:
214.1. înregistrarea incidentului;
214.2. evaluarea naturii și gravității acestuia;
214.3. limitarea efectelor și izolarea componentelor afectate;
214.4. conservarea urmelor și a probelor digitale relevante;
214.5. înlăturarea cauzelor incidentului;
214.6. restabilirea funcționării sistemului;
214.7. informarea subiecților implicați și notificarea autorităților competente, în cazurile și în condițiile prevăzute de actele normative.

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

216. 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, după caz, răspunderea disciplinară, contravențională, civilă sau penală, în condițiile legii.

217. Cerințele tehnice detaliate privind securitatea, jurnalizarea, monitorizarea, controlul, auditul, copiile de rezervă, asigurarea continuității activității, recuperarea în caz de dezastru și gestionarea incidentelor se stabilesc în 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. Elaborarea 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 cazurile, condițiile și limitele prevăzute expres de lege și, după caz, de actele normative adoptate în executarea acesteia, 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. Totodată, proiectul este elaborat în vederea punerii în aplicare a Legii nr. 209/2026 privind cooperarea polițienească internațională, care constituie cadrul legal general pentru căutarea și schimbul automatizat de date în scopul cooperării polițienești. Prezenta hotărâre nu instituie de sine stătător competențe noi de prelucrare a datelor biometrice în scopul schimbului automatizat transfrontalier, ci stabilește cadrul conceptual, organizatoric și procedural necesar pentru funcționarea Sistemului informațional „Registrul imaginilor faciale”, urmând ca aplicarea componentei de schimb automatizat transfrontalier al datelor de referință privind imaginile faciale să se realizeze numai după intrarea în vigoare a legii speciale și în condițiile stabilite de aceasta.
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 cazurile, condițiile și limitele prevăzute expres de lege și, după caz, de actele normative adoptate în executarea acesteia, 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 distincte 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 informaționale nu au ca obiect principal constituirea și administrarea unei evidențe specializate a imaginilor faciale ale bănuiților, învinuiților și condamnaților, a datelor de referință privind imaginile faciale ale acestora și a mecanismelor de comparare și validare a concordanțelor.

În ceea ce privește Sistemul informațional „Registrul de stat al populației", acesta are o finalitate juridică și funcțională diferită, fiind destinat evidenței populației, identificării persoanelor și gestionării datelor aferente statutului persoanei și actelor de identitate. Acest sistem nu are ca obiect principal gestionarea specializată a imaginilor faciale în scopuri polițienești, criminalistice, de căutare, de comparare biometrică facială, validare a concordanțelor, jurnalizare, audit, trasabilitate și cooperare polițienească internațională.

Prin urmare, Sistemului informațional „Registrul imaginilor faciale" nu substituie și nu dublează Registrul de stat al populației, ci instituie o resursă informațională specializată, cu regim juridic și funcțional distinct, destinată 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, dar și gestionării datelor de referință privind imaginile faciale în condiții de legalitate, necesitate, proporționalitate, limitare a scopului, minimizare a datelor, securitate, jurnalizare și trasabilitate. Interoperabilitatea cu Sistemul informațional „Registrul de stat al populației" și cu alte sisteme informaționale relevante se va realiza numai în măsura necesară îndeplinirii scopurilor prevăzute de actele normative privind cooperarea polițienească internațională, fără preluarea nejustificată sau duplicarea generalizată a datelor existente în sistemele-sursă.

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 domeniul prevenirii, constatării și investigării infracțiunilor, inclusiv pentru căutarea persoanelor dispărute și identificarea cadavrelor ori a părților acestora. În schimb, setul de date destinat schimbului automatizat transfrontalier trebuie să fie constituită distinct, 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.

Componenta națională și setul de date de referință destinat schimbului automatizat transfrontalier a Sistemului informațional „Registrul imaginilor faciale" au regimuri juridice și funcționale distincte. Componenta națională se utilizează pentru scopurile prevăzute de legislația națională aplicabilă, inclusiv prevenirea, constatarea și investigarea infracțiunilor, căutarea persoanelor dispărute și identificarea cadavrelor ori a părților acestora. Setul de date destinat schimbului automatizat transfrontalier reprezintă o componentă distinctă, limitată la categoriile de persoane prevăzute de Regulamentul (UE) 2024/982 și de Legea nr. 209/2026 privind cooperarea polițienească internațional, fără date care permit identificarea directă a persoanei.

De asemenea, o altă problemă constă în faptul că, 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 actului normativ 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"* 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 Sistemului informațional „Registrul imaginilor faciale", cu responsabilitatea de a asigura condițiile juridice, financiare și organizatorice necesare pentru crearea, administrarea, mentenanța și dezvoltarea sistemului. Serviciul Tehnologii Informaționale din subordinea Ministerului Afacerilor Interne are calitatea de deținător al Sistemului informațional „Registrul imaginilor faciale" 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" deține calitatea de administrator tehnic, care asigură administrarea tehnică și menținerea Sistemului informațional „Registrul imaginilor faciale" în conformitate cu Regulamentul privind administrarea tehnică și menținerea resurselor și sistemelor informaționale de stat, aprobat prin 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.

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 nr. 209/2026 privind cooperarea polițienească internațională 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 Sistemului informațional „Registrul imaginilor faciale" 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 reglementează modul de organizare, ținere, administrare, actualizare, utilizare, furnizare, protecție și arhivare a datelor din Registrul imaginilor faciale. Regulamentul detaliază subiecții raporturilor juridice aferente Registrului imaginilor faciale, 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*. Sistemul informațional „Registrul imaginilor faciale" 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 imaginile faciale, metadatele, informațiile asociate și rezultatele comparării automatizate necesare realizării atribuțiilor autorităților competente, exclusiv în condițiile legii și pentru scopuri determinate. Setul de date de referință destinat schimbului automatizat transfrontalier va reprezenta o submulțime distinctă a datelor gestionate în Registrul imaginilor faciale, constituită, păstrată, furnizată și utilizată numai în condițiile Regulamentului (UE) 2024/982, ale legii speciale privind cooperarea polițienească internațională și ale actelor normative adoptate în executarea acesteia

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 Registrul imaginilor faciale 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.

În ceea ce privește structura numărului de referință al imaginii faciale, proiectul delimitează numărul de referință utilizat pentru schimbul automatizat transfrontalier de elementele tehnice interne utilizate pentru administrarea Registrului imaginilor faciale prin intermediul Sistemului informațional „Registrul imaginilor faciale". Elementele tehnice interne, cum ar fi identificatorul unic intern al imaginii faciale, codul categoriei obiectului informațional, indicatorul statutului imaginii, elementul de versiune ori elementul tehnic de control al integrității, au exclusiv rol administrativ și tehnic. Acestea sunt necesare pentru individualizarea obiectului informațional în cadrul Sistemului informațional „Registrul imaginilor faciale", prevenirea dublării înregistrărilor, asigurarea trasabilității, integrității și corelării controlate cu metadatele, rezultatele comparării automatizate și înregistrările privind validarea concordanței.

Aceste elemente nu constituie date de identificare directă a persoanei și nu extind conținutul datelor de referință puse la dispoziție în cadrul schimbului automatizat transfrontalier.

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.

În cazul victimelor, includerea datelor de referință privind imaginile faciale în setul destinat schimbului automatizat transfrontalier se va realiza numai în cazurile, condițiile și limitele prevăzute expres de lege, cu respectarea principiilor legalității, necesității, proporționalității, limitării scopului, minimizării datelor și protecției datelor cu caracter personal. Această soluție exclude includerea automată sau generalizată a imaginilor victimelor în setul de date destinat schimbului transfrontalier.

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 Sistemului informațional „Registrul imaginilor faciale", 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 Registrul imaginilor faciale. Sistemul informațional „Registrul imaginilor faciale" 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 Sistemului informațional „Registrul imaginilor faciale" 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, Sistemul informațional „Registrul imaginilor faciale" utilizează, după caz, serviciile electronice guvernamentale partajate MPass, MSign, MLog, MNotify, MPower, cu respectarea cadrului normativ aplicabil, a cerințelor tehnice, de securitate și de trasabilitate.

La proiectarea și dezvoltarea interfețelor Sistemului informațional „Registrul imaginilor faciale" 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 Sistemului informațional „Registrul imaginilor faciale" 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.

Totodată, proiectul instituie o garanție de imparțialitate prin *stabilirea incompatibilității persoanei care a participat, în calitate de personal calificat, la validarea concordanței rezultate din compararea automatizată efectuată prin Sistemul informațional „Registrul imaginilor faciale”* de a participa ulterior, în aceeași cauză, în calitate de specialist sau expert judiciar, la examinarea, verificarea ori evaluarea aceluiași rezultat sau a aceleiași concordanțe

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 Hotărârea de Guvern să intre în vigoare la data intrării în vigoare a Legii nr. 209/2026 privind cooperarea polițienească internațională, pentru a asigura corelarea cu 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 a hotărârii de Guvern, dar numai în condițiile stabilite la pct. 5 din hotărâre, respectiv pe măsura îndeplinirii condițiilor 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.

În cadrul acestei opțiuni a fost analizată inclusiv posibilitatea utilizării Sistemului informațional „Registrul de stat al populației" ca sursă principală pentru imaginile faciale. Această opțiune nu a fost reținută, deoarece Registrul de stat al populației are o finalitate distinctă, orientată spre evidența populației și documentarea persoanelor, iar nu spre gestionarea specializată a imaginilor faciale în scopuri polițienești, criminalistice, de căutare, comparare biometrică facială, validare a concordanțelor, jurnalizare, audit și schimb automatizat transfrontalier de date de referință. Utilizarea exclusivă a Registrului de stat al populației nu ar permite instituirea unui regim diferențiat pentru imaginile neidentificate, datele de referință, listele de mostre, validarea concordanțelor, trasabilitatea operațiunilor și delimitarea setului destinat schimbului transfrontalier

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 Sistemului informațional „Registrul imaginilor faciale", 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 Sistemului informațional „Registrul imaginilor faciale” 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 Sistemului informațional „Registrul imaginilor faciale”.

Pentru Ministerul Afacerilor Interne, impactul va consta în consolidarea capacității instituționale de coordonare a proceselor aferente creării și utilizării Registrului imaginilor faciale, 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 din subordinea Ministerului Afacerilor Interne, în calitate de deținător al Sistemului informațional „Registrul imaginilor faciale”, 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.

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.

Sistemul informațional „Registrul imaginilor faciale” va fi găzduit pe Platforma tehnologică guvernamentală comună (MCloud), iar interoperabilitatea cu sistemele informaționale și resursele informaționale relevante ale statului se va realiza prin platforma MConnect și, după caz, prin MConnect Events, cu utilizarea serviciilor electronice guvernamentale partajate MPass, MSign, MLog, MNotify și MPower, în condițiile cadrului normativ aplicabil.

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, 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, implementării, administrării tehnice, mentenanței și asigurării funcționării Sistemului informațional „Registrul imaginilor faciale”.

Proiectul hotărârii Guvernului instituie cadrul normativ general pentru crearea și funcționarea Sistemului informațional „Registrul imaginilor faciale” și prevede că Ministerul Afacerilor Interne, în calitate de posesor al Sistemului informațional „Registrul imaginilor faciale”, va asigura condițiile juridice, financiare și organizatorice necesare pentru crearea, administrarea, mentenanța și dezvoltarea sistemului. Totodată, proiectul nu stabilește, prin sine, alocări bugetare imediate, acestea urmând a fi planificate etapizat, în funcție de documentația tehnică, caietul de sarcini, soluția tehnologică selectată, cerințele de securitate, interoperabilitate și mentenanță, precum și de disponibilitatea mijloacelor financiare.

Potrivit estimărilor tehnico-economice prezentate de Serviciul Tehnologii Informaționale din subordinea Ministerului Afacerilor Interne, pentru fundamentarea corespunzătoare a proiectului este necesară realizarea unei etape pregătitoare, care să includă elaborarea studiului de fezabilitate, efectuarea studiului de piață și elaborarea termenilor de referință/caietului de sarcini pentru achiziția lucrărilor și serviciilor necesare creării Sistemului informațional „Registrul imaginilor faciale”.

Costurile estimative pentru etapa pregătitoare sunt următoarele:

a) studiul de fezabilitate – 800–1.800 mii lei, fără TVA, cu o perioadă estimativă de realizare de 4–6 luni;

b) studiul de piață – 200–450 mii lei, fără TVA, cu o perioadă estimativă de realizare de 1,5–2,5 luni;

c) elaborarea termenilor de referință/caietului de sarcini – 400–900 mii lei, fără TVA, cu o perioadă estimativă de realizare de 2,5–4 luni.

Astfel, costul estimativ total al etapei pregătitoare constituie 1.400–3.150 mii lei, fără TVA, cu o perioadă estimativă agregată de realizare de 6–9 luni, ținând cont de posibilitatea desfășurării parțial paralele a activităților menționate.

Urmare a dării în exploatare a Sistemului informațional „Registrul imaginilor faciale”, posesorul va încheia cu administratorul tehnic acordul privind administrarea tehnică și menținerea Sistemului informațional „Registrul imaginilor faciale”, care va include activitățile minime privind administrarea tehnică și menținerea sistemului, precum și volumul acestora. În baza acordului vor fi estimate cheltuielile aferente administrării tehnice și menținerii Sistemului informațional „Registrul imaginilor faciale”, care urmează a fi acoperite în condițiile cadrului

bugetar aplicabil, în limita mijloacelor financiare aprobate anual și, după caz, din alte surse neinterzise de lege.

Costurile finale aferente dezvoltării, implementării, administrării tehnice, mentenanței și funcționării Sistemului informațional „Registrul imaginilor faciale" vor putea fi determinate cu exactitate după finalizarea studiului de fezabilitate, a studiului de piață și a termenilor de referință/caietului de sarcini. Aceste documente vor stabili cerințele funcționale și nefuncționale, arhitectura tehnică, cerințele de interoperabilitate, cerințele de securitate informațională și securitate cibernetică, cerințele privind protecția datelor cu caracter personal, indicatorii de performanță, condițiile de testare, acceptanță, administrare tehnică și mentenanță.

Costurile aferente implementării Sistemului informațional „Registrul imaginilor faciale" vor viza, în principal:

a) elaborarea și aprobarea documentației tehnice aferente sistemului;

b) dezvoltarea sau achiziționarea soluției informatice necesare funcționării Sistemului informațional „Registrul imaginilor faciale";

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 poate genera costuri suplimentare distincte, aferente conectării la infrastructuri și mecanisme externe, configurării interfețelor tehnice, asigurării cerințelor de securitate și interoperabilitate, efectuării testărilor tehnice și implementării actelor de punere în aplicare aplicabile. Aceste costuri vor putea fi determinate după clarificarea condițiilor juridice, organizatorice și tehnice necesare operaționalizării schimbului transfrontalier, inclusiv cu luarea în considerare a Deciziei de punere în aplicare (UE) 2026/1064, a cerințelor tehnice aplicabile mecanismului Prüm și a eventualelor acte de punere în aplicare ori specificații tehnice ulterioare relevante.

Finanțarea măsurilor aferente creării, dezvoltării, implementării, administrării tehnice, mentenanței și funcționării Sistemului informațional „Registrul imaginilor faciale" va fi realizată din contul și în limitele mijloacelor financiare aprobate anual în bugetul Ministerului Afacerilor Interne și al instituțiilor din subordine, precum și, după caz, din alte surse neinterzise de lege, inclusiv proiecte de asistență externă, programe de suport tehnic sau alte mecanisme financiare aferente procesului de modernizare instituțională și integrare europeană.

Totodată, având în vedere relevanța proiectului pentru procesul de integrare europeană și alinierea la acquis-ul Uniunii Europene în domeniul cooperării polițienești și schimbului automatizat de date, poate fi examinată posibilitatea atragerii finanțării externe, inclusiv prin programe și proiecte susținute de Uniunea Europeană, Banca Mondială, UNDP, GIZ sau alți parteneri de dezvoltare.

Prin urmare, aprobarea proiectului hotărârii Guvernului *nu instituie cheltuieli imediate peste alocațiile bugetare aprobate, însă creează cadrul normativ necesar pentru planificarea etapizată a resurselor financiare aferente dezvoltării și funcționării Sistemului informațional „Registrul imaginilor faciale"*. 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 Sistemului informațional „Registrul imaginilor faciale", 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 Sistemului informațional „Registrul imaginilor faciale", 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 Sistemului informațional „Registrul imaginilor faciale" 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 Sistemului informațional „Registrul imaginilor faciale”.

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 Sistemului informațional „Registrul imaginilor faciale”.

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 Sistemului informațional „Registrul imaginilor faciale” 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 Registrul imaginilor faciale 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 Sistemului informațional „Registrul imaginilor faciale”, 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 Sistemului informațional „Registrul imaginilor faciale”, 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 Sistemului informațional „Registrul imaginilor faciale" 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 Sistemului informațional „Registrul imaginilor faciale" 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 punerea în aplicare 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 punerea în aplicare 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.

Prin proiect se asigură punerea în aplicare parțială, la nivel național, a art. 19–24 din Regulamentul (UE) 2024/982, în partea referitoare la datele de referință privind imaginile faciale și căutarea automatizată a acestora. Proiectul stabilește cadrul intern necesar pentru organizarea, ținerea și funcționarea Registrului imaginilor faciale, constituirea setului de date de referință, excluderea datelor care permit identificarea directă a persoanei din setul destinat schimbului transfrontalier, utilizarea numerelor de referință, validarea umană a concordanțelor, securitatea, jurnalizarea și trasabilitatea operațiunilor.

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 Sistemul informațional „Registrul imaginilor faciale” 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 Sistemului informațional „Registrul imaginilor faciale” IF 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 Sistemului informațional „Registrul imaginilor faciale” 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.

Cerințele tehnice, formatele de date, protocoalele de comunicare, mecanismele de securitate, jurnalizare, trasabilitate și disponibilitate aferente componentei de schimb automatizat transfrontalier al datelor de referință privind imaginile faciale urmează a fi stabilite prin documentația tehnică a Sistemului informațional „Registrul imaginilor faciale”, cu respectarea Regulamentului (UE) 2024/982, a Deciziei de punere în aplicare (UE) 2026/1064 și a standardelor europene și internaționale aplicabile

Aplicarea efectivă a prevederilor privind schimbul automatizat transfrontalier al datelor de referință privind imaginile faciale va avea loc numai după intrarea în vigoare a legii privind cooperarea polițienească internațională și după îndeplinirea condițiilor juridice, organizatorice și tehnice prevăzute de aceasta. Până la acel moment, proiectul stabilește cadrul național conceptual și organizatoric necesar pentru dezvoltarea Sistemului informațional „Registrul imaginilor faciale” și pentru pregătirea aplicării ulterioare a mecanismului de schimb automatizat.

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 și consultare publică a 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.

În vederea asigurării transparenței procesului decizional, precum și pentru definitivarea unui cadru normativ coerent, aplicabil și echilibrat, la 18 septembrie 2026, Ministerul Afacerilor Interne a organizat o ședință de consultare publică în regim online.

Lista autorităților și instituțiilor care au participat 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. Ministerul Afacerilor Externe;
5. Ministerul Muncii și Protecției Sociale;
6. Agenția de Guvernare Electronică;
7. Centrul Național pentru Protecția Datelor cu Caracter Personal;
8. Agenția Servicii Publice;
9. Procuratura Generală;
10. Serviciul de Informații și Securitate;
11. Serviciul Tehnologia Informației și Securitate Cibernetică.
12. Centrul Național Anticorupție;
13. Oficiul Avocatului Poporului.

Expertize:

1. Ministerul Justiției;
2. Centrul Național Anticorupție;
3. Centrul de Armonizare a Legislației.

Propunerile și obiecțiile formulate de autoritățile și instituțiile participante în procesul de avizare au fost incluse în sinteză și luate în considerare în procesul de definitivare a proiectului de hotărâre.

7. Concluziile expertizelor

Propunerile parvenite în procesul de expertiză de compatibilitate, formulate de Centrul de Armonizare a Legislației (aviz nr. 31/02-69-7670 din 30.06.2026) au fost luate în considerare la definitivarea proiectului și incluse în sinteză.

În conformitate cu raportul de expertiză juridică Ministerul Justiției (nr. 04/1-8797 din 03.08.2026) au fost înaintate o serie de propuneri în privința proiectului, care au fost luate în considerare la definitivarea proiectului de lege și incluse în sinteză.

În conformitate cu expertiza anticorupție efectuată de către Centrul Național Anticorupție (raport de expertiză anticorupție nr. EHG26/11723 din 27.07.2026) s-a constatat că proiectul a fost elaborat de către Ministerul Afacerilor Interne promovează interesul public manifestat prin instituirea Sistemului informațional „Registrul imaginilor faciale” în vederea racordării cadrului legal la normele comunitare în domeniu.

8. Modul de încorporare a actului în cadrul normativ existent

Proiectul se încadrează în cadrul normativ existent și nu implică, la etapa aprobării, modificarea concomitentă a altor acte normative. Implementarea Sistemului informațional „Registrul imaginilor faciale” va necesita elaborarea documentației tehnice, aprobarea procedurilor operaționale interne și, după caz, ajustarea sau aprobarea unor acte normative subsecvente necesare funcționării sistemului.

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 Sistemului informațional „Registrul imaginilor faciale”. Ministerul Afacerilor Interne, în calitate de posesor al sistemului, va coordona procesul de implementare. Serviciul Tehnologii Informaționale din subordinea Ministerului Afacerilor Interne, în calitate de deținător al Sistemului informațional „Registrul imaginilor faciale”, 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” va exercita atribuțiile ce țin de administrarea tehnică și menținerea Sistemului informațional „Registrul imaginilor faciale” în condițiile Regulamentului privind administrarea tehnică și menținerea resurselor și sistemelor informaționale de stat, aprobat prin 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, precum și ale acordului privind administrarea tehnică și menținerea Sistemului informațional „Registrul imaginilor faciale”.

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 al datelor de referință va fi implementată etapizat, numai după intrarea în vigoare a Legii nr. 209/2016 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.

Ministru **Daniella MISAIL-NICHITIN**

Digitally signed by Misail-Nichitin Daniella
Date: 2026.09.30 20:00:04 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

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 (număr unic 620/MAI/2026)

Participantul la avizare, consultare publică, expertizare	Nr. crt.	Conținutul obiecției, propunerii, recomandării, concluziei	Argumentarea autorului proiectului
Procedura de avizare			
Ministerul Dezvoltării Economice și Digitalizării (aviz nr. 13/2-2122 din 23.06.2026)	**1.**	La Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale La Capitolul II -VII Informăm că în Regulamentul expus spre avizare se constată utilizarea improprie a sintagmei Registrului imaginilor faciale în contexte care vizează de fapt funcționalitățile tehnice ale Sistemului informațional „Registrul imaginilor faciale”, aspecte reglementate distinct prin Conceptul SI RIF. Cu titlu de informate, precizăm că conform prevederilor art. 3 al Legii nr. 467/2003, resursă informațională este totalitate de informații documentate în sistemele informaționale automatizate, organizată în conformitate cu cerințele stabilite și cu legislația în vigoare, în timp ce sistemul informațional constituie infrastructura (tehnologii, metode, personal) destinată gestionării acestei informații. Deși cele două entități sunt interdependente, ele sunt distincte din punct de vedere funcțional și juridic. Totodată, potrivit prevederilor art. 3 al Legii nr. 71/2007 cu privire la registre, registrul este totalitatea informațiilor documentate ținute în sisteme informaționale automatizate, organizată în conformitate cu cerințele stabilite și cu legea. Subsecvent, articolul 76 al Legii nr. 467/2003 menționează expres care sunt documentele sistemelor și resurselor informaționale de stat: conceptul sistemului informațional,	**Se acceptă.** Proiectul a fost revizuit prin delimitarea terminologică și funcțională dintre Sistemul informațional „Registrul imaginilor faciale” și Registrul imaginilor faciale, în calitate de resursă informațională departamentală de stat. În Regulament au fost ajustate formulările care atribuiau Registrului funcționalități tehnice proprii sistemului informațional.

		caietul de sarcini al sistemului informațional și regulamentul resursei informaționale, care conține: -reglementări privind drepturile și obligațiile subiecților raporturilor juridice aferente creării și ținerii resursei informaționale; -modalitatea de ținere a resursei informaționale; -procedura de înregistrare, modificare, completare și radiere a datelor; -procedura de interacțiune cu furnizorii de date; -măsuri privind asigurarea securității resursei informaționale. În contextul celor expuse, reiterăm că Regulamentul nu este conform sub aspectul obiectului de reglementare, deoarece deși titlul face referire la resursa informațională formată de SI RIF, obiectul reglementat, de fapt, este Registrul imaginilor faciale. În concluzie, în contextul prevederilor art. 1 al Legii nr. 71/2007, informăm că proiectul Regulamentului Registrului imaginilor faciale expus spre avizare nu este conform și urmează a fi aliniat cadrului normativ aplicabil registrelor, delimitând reglementările ce vizează resursa informațională vis-a-vis de sistemul de gestiune aferent.	
Ministerul Finanțelor (aviz nr. 07/4-03/231/1036 din 26 iunie 2026)	**2.**	La proiectul de hotărâre. Se propune de completat cu un punct nou care să reglementeze sursa de finanțare pentru dezvoltarea, administrarea mentenanța și funcționarea sistemului informațional. Această completare este fundamentată pe normele imperative ale Legii nr. 100/2017 cu privire la actele normative, fiind coroborată cu principiile responsabilității bugetar-fiscale statuate prin Legea finanțelor publice și responsabilității bugetar fiscale nr. 181/2014, potrivit cărora orice propunere cu impact financiar trebuie să aibă o sursă bugetară clar determinată.	**Se acceptă.**

	3.	La Conceptul Sistemului informațional „Registrul imaginilor faciale” din anexa nr. 1 la proiectul de hotărâre. Pct. 19, subpct. 19.19. se exclude, întrucât 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 personala, este deja caducă, fiind abrogată prin Hotărârea Guvernului nr. 678/2024 cu privire la modificarea și abrogarea unor hotărâri ale Guvernului (facilitarea activității mediului de afaceri VI). Totodată, se propune de completat cu un subpunct nou care va avea următorul conținut: „Ordinul Ministerului Dezvoltării Informaționale nr. 78/2006 cu privire la aprobarea reglementării tehnice „Procesele ciclului de viață al software-ului” RT 38370656-002:2006”. Această modificare este necesară întrucât prezenta reglementare tehnică se referă la procesele ciclului de viață al software- ului și este obligatorie la crearea tuturor sistemelor informaționale automatizate de importanță statală.	**Se acceptă.**
	4.	La Nota de fundamentare. Deși, în pct. 4.2. „Impactul financiar și argumentarea costurilor estimative” se menționează că implementarea proiectului de hotărâre nu va avea impact financiar suplimentar asupra bugetului de stat, iar dezvoltarea și mentenanța sistemului informațional urmează a fi asigurate în limitele bugetului de stat aprobat anual, autorul urmează să specifice nemijlocit costul estimativ al dezvoltării și mentenanței sistemului informațional, în vederea asigurării transparenței procesului de planificare bugetară și a evaluării impactului financiar real al proiectului.	**Se acceptă.**
Procuratura Generală (aviz nr.	**5.**	Cu privire la includerea imaginilor faciale ale victimelor în setul de date de referință destinat schimbului automatizat transfrontalier Potrivit pct. 56 din Regulament, setul de date de	**Se acceptă parțial.** Proiectul hotărârii de Guvern are caracter subsecvent și derivă din proiectul de lege privind

nr.4-1d/26-429 din 26.06.2026)		referință privind imaginile faciale destinat schimbului automatizat transfrontalier se constituie 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 măsura în care cadrul normativ național permite acest lucru. Considerăm că sintagma „precum și, după caz, ale victimei, în măsura în care cadrul normativ național permite acest lucru” este formulată excesiv de general și nu permite identificarea situațiilor concrete în care imaginile faciale ale victimelor pot fi introduse în setul de date de referință destinat schimbului automatizat transfrontalier. în lipsa unor criterii clare privind necesitatea, proporționalitatea și scopul unei asemenea prelucrări, norma poate genera ingerințe disproporționate în dreptul la viață privată și în dreptul la protecția datelor cu caracter personal ale persoanelor care nu sunt vizate de suspiciuni privind săvârșirea unor infracțiuni. în acest context, se recomandă reexaminarea normei prin excluderea categoriei respective de persoane sau, cel puțin, prin reglementarea expresă și limitativă a situațiilor în care imaginile faciale ale victimelor pot fi incluse în setul de date de referință destinat schimbului automatizat transfrontalier.	cooperarea polițienească internațională (număr unic 264/MAI/2026), care constituie actul normativ de nivel superior în raport cu prezentul proiect. În acest sens, hotărârea Guvernului nu poate exclude, restrânge sau modifica categoriile de date și persoane prevăzute de lege, cu privire la datele de referință cu privire la imaginile faciale, care fac obiectul schimbului transfrontalier de informații. Se menționează că art. 18 alin. (1) din proiectul de lege menționat supra prevede că, 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*. Totodată, în contextul observației privind claritatea, previzibilitatea și proporționalitatea prelucrării datelor biometrice ale victimelor, formularea din proiect a fost revizuită, astfel încât să rezulte expres că datele de referință privind imaginile faciale ale victimelor pot fi incluse în setul de date destinat schimbului automatizat transfrontalier numai în cazurile, condițiile și limitele prevăzute expres de lege, cu respectarea principiilor necesității, proporționalității, limitării scopului și protecției datelor cu caracter personal (pct. 10.3 din Concept și pct. 50-51 din Regulament).
	6.	Cu privire la termenele de păstrare a imaginilor faciale Analizând prevederile pct. 69 și pct. 71 din Regulament, constatăm că proiectul stabilește doar principiul păstrării diferențiate a datelor, fără a prevedea termene concrete de	**Se acceptă.** Proiectul a fost completat prin revizuirea Capitolului IV, Secțiunea a 4-a, în special pct. 65–70 din Regulament, în vederea stabilirii unui regim

		stocare pentru diferitele categorii de imagini faciale și date biometrice gestionate prin SI RIF. Or, având în vedere caracterul sensibil al datelor biometrice și exigențele principiului limitării stocării, durata păstrării datelor trebuie să fie previzibilă, determinabilă și proporțională cu scopul prelucrării. în aceste condiții, considerăm necesară completarea proiectului cu reglementări care să stabilească termene clare de păstrare a imaginilor faciale și a datelor asociate, diferențiate în funcție de categoria persoanei vizate, scopul prelucrării și statutul procedurilor relevante, precum și condițiile și criteriile care justifică eventuala prelungire a acestor termene.	mai clar și determinabil al termenelor de păstrare a imaginilor faciale, datelor de referință, metadatelor, rezultatelor comparării automatizate și evidențelor de jurnalizare. Au fost introduse criterii diferențiate în funcție de categoria persoanei vizate, categoria obiectului informațional, scopul prelucrării, statutul cauzei penale, al dosarului de căutare ori al altei proceduri relevante, precum și condițiile de prelungire motivată a termenului de păstrare. Totodată, termenele concrete aplicabile fiecărei categorii de date urmează a fi reflectate în nomenclatorul documentelor și în procedurile interne aprobate în condițiile legii, întrucât acestea trebuie corelate cu legislația procesual-penală, legislația privind arhivarea, actele normative speciale aplicabile și statutul concret al fiecărei proceduri.
	7.	Cu privire la statutul Procuraturii în cadrul Sistemului informațional „Registrul imaginilor faciale” Proiectul reglementează categoriile de destinatari ai datelor din Registrul imaginilor faciale, însă nu stabilește expres statutul Procuraturii în cadrul acestui sistem informațional și nici modalitatea de acces la rezultatele comparărilor biometrice validate. în același timp, SI RIF este destinat inclusiv prevenirii, constatării și investigării infracțiunilor, iar rezultatele comparărilor biometrice pot constitui informații relevante pentru activitatea de urmărire penală. Ținând cont de atribuțiile constituționale și legale ale procurorului privind conducerea și exercitarea urmăririi penale, considerăm necesară reglementarea expresă a statutului Procuraturii în cadrul SI RIF, inclusiv prin includerea acesteia în categoria destinatarilor datelor, precum și prin stabilirea	**Se acceptă.**

		mecanismului de acces la rezultatele comparărilor biometrice validate și la informațiile asociate acestora, în condițiile legii. O asemenea precizare ar contribui la asigurarea exercitării efective a atribuțiilor procurorului în cadrul procesului penal și la valorificarea corespunzătoare a informațiilor obținute prin intermediul sistemului.	
	8.	În concluzie, Procuratura Generală recomandă examinarea oportunității valorificării observațiilor și propunerilor formulate în prezentul aviz, în vederea consolidării garanțiilor privind protecția datelor cu caracter personal, asigurării previzibilității regimului de păstrare a datelor biometrice și clarificării rolului Procuraturii în procesul de utilizare a rezultatelor generate de Sistemul informațional „Registrul imaginilor faciale”.	**S-a luat act.**
Agenția Servicii Publice (aviz nr. nr. 01/6003 din 29.06.2026)	**9.**	La Anexa 1 (Conceptul Sistemului informațional) 1. La punctul 19: - subpct. 19.19, se propune de exclus, întrucât 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 a fost abrogată prin Hotărârea Guvernului nr. 678/2024; - se propune de completat cu subpunctele 19.35 – 19.38 cu următorul conținut: „19.35 Reglementarea tehnică „Procesele ciclului de viață al software-ului” RT 38370656-002:2006, aprobată prin Ordinul Ministrului dezvoltării informaționale nr. 78/2006; 19.36 Standardul Republicii Moldova SM ISO/CEI 12207:2014 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al software-ului”; 19.37 Standardul Republicii Moldova SM ISO/CEI/IEEE 15288:2015 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al software-ului”;	**Se acceptă.**

		19.38 Standardul Republicii Moldova SM ISO/CEI 27002:2017 „Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației.”	
	10.	Se constată o dublare a conținutului dintre pct. 38-45 din Concept și pct. 11-20 din Regulament, ceea ce contravine principiilor de tehnică legislativă privind paralelismele normative în cadrul aceluiași act normativ, prevăzute la art. 54 alin. (1) lit. g), art. 55 alin. (4) și art. 65 alin. (2) lit. d) din Legea nr. 100/2017. Potrivit art. 9–15 din Legea nr.71/2007 și pct.2.2.5. din Anexa nr. 3 la RT 38370656 – 002:2006, Conceptul trebuie să conțină descrierea detaliată a tuturor participanților la procesul informațional și a funcțiilor specifice exercitate de aceștia, inclusiv privind înregistrarea datelor în registru. În acest context, Regulamentul urmează să fie restructurat astfel încât să conțină exclusiv drepturile și obligațiile subiecților raporturilor juridice, fără repetarea descrierilor funcționale ce țin de conținutul Conceptului.	**Se acceptă.**
	11.	Pct. 60 din Concept urmează să fie reformulat. Contrar cerințelor de structură stabilite în Anexa nr. 3, pct. 2.2.7 din RT 38370656 – 002:2006, proiectul deleagă stabilirea structurii identificatorilor către Regulament. Or, norma tehnică menționată stabilește imperativ că structura identificatorului fiecărui obiect informațional trebuie să fie descrisă în Concept, întrucât aceasta determină unicitatea și modalitatea de regăsire a datelor în spațiul informațional. În acest sens, se solicită includerea descrierii structurii identificatorilor în textul Conceptului și excluderea normelor corespunzătoare din Regulament.	**Se acceptă.**
	12.	Pct. 76 urmează să fie revizuit în vederea detalierii fluxurilor de date pentru fiecare sistem sursă menționat. Conform pct.2.2.7 din Anexa nr. 3 la RT 38370656 – 002:2006,	**Se acceptă.**

		Conceptul trebuie să descrie explicit seturile de date ce vor fi preluate din fiecare registru nominalizat (de exemplu: din Registrul de stat al populației – date cu caracter personal ale persoanelor fizice luate la evidență; din Registrul dactiloscopic – date dactiloscopice, date cu caracter personal și date despre caz etc.).	
	13.	Se recomandă revizuirea terminologică a proiectului prin substituirea sintagmelor „prevăzute de lege”, „permise de lege” sau „în condițiile legii” cu sintagma mai largă „prevăzute de actele normative”. Această ajustare este necesară în conformitate cu art. 2, art. 6 și art. 54 alin. (1) lit. c) din Legea nr. 100/2017, pentru a asigura includerea întregului spectru de acte normative (legi, hotărâri de Guvern, acte normative ale autorităților publice etc.) care reglementează aspectele tehnice și organizaționale ale sistemului.	**Se acceptă.**
	14.	La Anexa 2 (Regulament privind modalitatea de ținere a Registrului imaginilor faciale) Secțiunea 3 Drepturile și obligațiile administratorului tehnic al RIF din Capitolul III. Drepturile și obligaţiile subiecţilor la crearea, exploatarea şi utilizarea RIF – de exclus.	**Se acceptă.**
Ministerul Afacerilor Externe (aviz nr. DI/3/041.1-7541 din 29 iunie 2026)	**15.**	La pct. 80.6 din proiectul de Concept, sintagma „acordurile și aranjamentele” urmează a fi eliminată dacă aceasta se referă la tratate internaționale (având în vedere că termenul „tratatele internaționale” a fost deja utilizat la punctul în cauză), ori înlocuită cu expresia „înțelegeri neguvernate de normele dreptului internațional public”, în cazul în care aceasta nu se încadrează în noțiunea de „tratat internațional”.	**Se acceptă.**
Oficiul Avocatului Poporului (opinie nr. 04-3/43-1652 din 30.06.2026)	**16.**	Conceptul Sistemului informațional „Registrul imaginilor faciale” 1) Lipsa distincției între categoriile procesuale ale persoanelor vizate Punctul 10.3 din proiectul Conceptului și prevederile similare din Regulamentul SI RIF reglementează introducerea	**Se acceptă parțial.** Proiectul a fost revizuit în vederea instituirii unei distincții mai clare între categoriile de persoane vizate și regimurile aferente de prelucrare, păstrare și utilizare a imaginilor faciale și a datelor de referință. Astfel, în Concept și Regulament se

		în registru a imaginilor faciale aparținând persoanelor identificate (bănuiți, învinuiți, inculpați, condamnați) și victimele „ în măsură în care cadrul normativ național permite acest lucru”, precum și a imaginilor faciale neidentificate colectate în cursul urmăririi penale sau al căutării persoanelor dispărute. Aceste prevederi ar putea intra în coliziune cu principiile prevăzute de art. 5 alin. (1) lit. b) și e) din Legea nr. 195/2024 care prevede că datele necesită a fi colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri și păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă ce nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele. De asemenea, art.9 din Legea nr. 195/2024 prevede prelucrarea categoriilor speciale de date cu caracter personal, doar în anumite situații argumentate. Sintagma „în măsura în care cadrul normativ național permite acest lucru”, utilizată în privința imaginilor victimelor, constituie o normă de trimitere, lipsită de previzibilitate, contrar art. 23 alin. (2) din Constituție ce presupune respectarea principiului accesibilității și previzibilității actelor normative. Este necesar de a stabili o distincție clară între datele cu caracter personal ale diferitelor categorii de persoane vizate. Această clasificare procesuală este necesară pentru a preveni aplicarea aceluiași regim de stocare și prelucrare persoanelor condamnate, bănuiților și, respectiv, persoanelor care nu sunt acuzate de nicio infracțiune. Propunere: Redactarea punctului 10 din Concept astfel încât să instituie regimuri distincte de stocare și prelucrare a imaginilor faciale, diferențiate după calitatea procesuală a subiecților precum și interdicția preclucrării categoriilor speciale de date cu caracter personal.	precizează că datele privind persoanele care au calitatea de bănuit, învinuit, inculpat, persoanele condamnate, victimele, persoanele dispărute, cadavrele ori părțile acestora, precum și imaginile faciale neidentificate se gestionează potrivit unor temeiuri, scopuri și condiții distincte, cu respectarea principiilor necesității, proporționalității, limitării scopului, minimizării datelor și limitării stocării. Proiectul hotărârii de Guvern are caracter subsecvent și derivă din proiectul de lege privind cooperarea polițienească internațională (număr unic 264/MAI/2026), care constituie actul normativ de nivel superior în raport cu prezentul proiect. În acest sens, hotărârea Guvernului nu poate exclude, restrânge sau modifica categoriile de date și persoane prevăzute de lege, cu privire la datele de referință cu privire la imaginile faciale, care fac obiectul schimbului transfrontalier de informații. Se menționează că art. 18 alin. (1) din proiectul de lege menționat supra prevede că, 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*. Totodată, în contextul observației privind claritatea, previzibilitatea și proporționalitatea prelucrării datelor biometrice ale victimelor, formularea din proiect a fost revizuită, astfel încât să rezulte expres că datele de referință privind imaginile faciale ale victimelor pot fi incluse în setul de date destinat schimbului automatizat

			transfrontalier numai în cazurile, condițiile și limitele prevăzute expres de lege, cu respectarea principiilor necesității, proporționalității, limitării scopului și protecției datelor cu caracter personal (pct. 10.3 din Concept și pct. 50-51 din Regulament). Totodată, nu se acceptă propunerea în partea ce ar presupune instituirea unei interdicții generale de prelucrare a datelor biometrice, întrucât obiectul proiectului constă tocmai în reglementarea prelucrării imaginilor faciale în scopuri determinate, legitime și prevăzute de lege. Pentru consolidarea garanțiilor, se introduce interdicția prelucrării categoriilor speciale de date cu caracter personal în afara cazurilor, condițiilor și limitelor prevăzute de lege și de actele normative adoptate în executarea acesteia.
	17.	2) La Capitolul III deficiențe ale cadrului normativ de referință și garanțiile instituționale. a) Sintagma „spațiu juridico-normativ” nu are corespondent în tehnica legislativă națională sau în standardele terminologice ale Legii nr. 100/2017 privind actele normative. Se recomandă reformularea titlului „Cadrul normativ aplicabil” sau „Temeiul juridic al funcționării SI RIF”.	**Se acceptă.**
	18.	b) Capitolul face trimitere generică la „tratatele internaționale”, fără a le enumera. Potrivit art. 4 din Constituție, tratatele internaționale privind drepturile omului au prioritate față de legislația internă. Prin urmare, se impune indicarea expresă a actelor internaționale transpuse sau aplicate. Se propune menționarea explicită a CEDO; Convenției Consiliului Europei nr. 108+ privind protecția persoanelor față de prelucrarea automatizată a datelor cu caracter personal.	**Se acceptă.**

	19.	c) Potrivit art. 35 din Legea nr. 195/2024, operatorul are obligația de a efectua o evaluare a impactului asupra protecției datelor înainte de orice operațiune de prelucrare susceptibilă să genereze riscuri ridicate pentru drepturile persoanelor vizate — categorie în care prelucrarea la scară largă a datelor biometrice se înscrie în mod neechivoc. Astfel, se propune introducerea unui punct nou ca înainte de punerea în exploatare a SI RIF și în cazul oricăror modificări semnificative ale sistemului, efectuarea unei evaluări a impactului asupra protecției datelor, în condițiile art. 35 din Legea nr. 195/2024, cu consultarea prealabilă a CNPDCP.	**Se acceptă.** Această prevedere este inclusă la pct. 185 din Regulament.
	20.	d) Potrivit Comisiei de la Veneția (CDL-AD(2025)054), utilizarea sistemelor de inteligență artificială de către autoritățile publice trebuie însoțită de garanții explicite împotriva utilizării excesive. În cauza Gluhin împotriva Rusiei (2023), CtEDO a reținut că utilizarea recunoașterii faciale impune cel mai înalt nivel de justificare și norme detaliate privind domeniul de aplicare. Se propune introducerea unui punct, ca SI RIF nu poate fi utilizat pentru supravegherea generalizată, monitorizarea permanentă sau identificarea nediferențiată a persoanelor în spații publice, cu excepția cazurilor expres prevăzute de lege și supuse autorizării judiciare prealabile și garanțiilor procedurale corespunzătoare.	**Nu se acceptă.** SI RIF nu este conceput ca un sistem de supraveghere video în timp real sau de monitorizare a spațiilor publice și identificarea în masă a persoanelor, însă ca sistem informațional specializat pentru evidența, compararea biometrică facială, validarea concordanțelor și gestionarea imaginilor faciale în scopul cooperării polițienești internaționale, în condițiile legii. Conceptul definește SI RIF ca sistem distinct specializat, destinat administrării și utilizării informațiilor privind imaginile faciale și datele de referință, inclusiv pentru schimb automatizat, iar nu ca infrastructură de supraveghere publică. Regulamentul prevede că operațiunile asupra datelor din RIF se efectuează numai de utilizatori autorizați, pe baza rolurilor atribuite, cu respectarea legalității, necesității, proporționalității, limitării scopului, securității și trasabilității. De asemenea, orice operațiune asupra datelor trebuie justificată prin scop legal, întemeiată pe

			documente/date/informații din surse autorizate și limitată la datele strict necesare realizării scopului. Prin urmare, completarea propusă nu este necesară în cadrul prezentului proiect și ar putea crea confuzie între SI RIF, ca sistem informațional de gestiune și comparare a datelor de referință privind imaginile faciale, și sistemele de supraveghere video ori recunoaștere facială în timp real, care nu constituie obiectul de reglementare al proiectului.
	21.	e) Se propune introducerea ca algoritmii utilizați în cadrul SI RIF sunt supuși evaluărilor periodice privind acuratețea, fiabilitatea și absența discriminării, iar rezultatele acestor evaluări sunt documentate și puse la dispoziția CNPDCP; Funcționarea SI RIF să fie supusă auditului periodic independent privind legalitatea prelucrării datelor, securitatea informațională și respectarea drepturilor fundamentale ale persoanelor vizate	**Nu se acceptă.** Propunerea nu se acceptă, întrucât proiectul conține deja mecanisme generale privind securitatea, jurnalizarea, monitorizarea, controlul și auditul SI RIF. Potrivit proiectului, componenta de jurnalizare, monitorizare și audit asigură evidența operațiunilor efectuate în sistem, trasabilitatea prelucrărilor, monitorizarea utilizării sistemului și suportul pentru controlul intern și audit, iar măsurile de securitate, jurnalizare, monitorizare, control și audit se aplică întregului ciclu de viață al datelor gestionate prin SI RIF. Aceste elemente urmează a fi stabilite la etapa elaborării studiului de fezabilitate, a caietului de sarcini, a specificațiilor tehnice și a procedurilor de testare, acceptanță, mentenanță și audit, cu luarea în considerare a standardelor tehnice aplicabile, inclusiv ICAO și ISO/IEC relevante. În partea ce ține de punerea rezultatelor evaluărilor la dispoziția Centrului Național pentru Protecția Datelor cu Caracter Personal, aceasta se realizează în condițiile competențelor legale ale

			autorității de supraveghere și ale legislației privind protecția datelor cu caracter personal, fără a fi necesară instituirea unei norme speciale suplimentare în prezentul proiect. De asemenea, impunerea caracterului „independent” al oricărui audit periodic nu este oportună la nivelul prezentului Regulament, deoarece auditul poate avea caracter intern, tehnic, de securitate cibernetică, de conformitate sau extern, în funcție de obiectul verificării și de cadrul normativ aplicabil.
	22.	f) Capitolul nu menționează drepturile cetățenilor în raport cu SI RIF. Se propune introducerea unor prevederi, ca persoanele vizate să beneficieze de un set de drepturi, ca dreptul la informare, acces, rectificare, ștergere, restricționarea prelucrării, opoziție și contestarea deciziilor individuale automatizate.	**Se acceptă.** Proiectul a fost completat cu pct. 106 din Regulament.
	23.	3) Riscul supravegherii biometrice a participanților la întruniri publice Pct. 32.1 prevede colectarea și recepționarea imaginilor faciale și a datelor de referință privind imaginile faciale. Prin urmare, considerăm că scanarea facială automată spre exemplu a protestatarilor pașnici ar putea genera un efect de descurajare care inhibă participarea cetățenilor la viața democratică a statului, fără a stabili restricții privind contextele de utilizare în timp real. Avocatul Poporului consideră că absența unor limite exprese creează riscul utilizării SI RIF pentru identificarea automată a participanților la întruniri publice, proteste sau manifestații pașnice. Art. 4 din Legea nr. 195/2024 definește „datele biometrice” incluzând expres imaginile faciale, iar art. 9 alin. (1) interzice, ca regulă generală, prelucrarea acestora pentru identificarea unică, cu excepția unor cazuri strict reglementate.	**Nu se acceptă.** Propunerea nu se acceptă, întrucât proiectul hotărârii Guvernului nu instituie un sistem de supraveghere video în timp real, de monitorizare a spațiilor publice sau de identificare biometrică nediferențiată a participanților la întruniri publice, proteste ori evenimente publice. SI RIF este conceput ca sistem informațional specializat pentru ținerea Registrului imaginilor faciale, gestionarea imaginilor faciale și a datelor de referință, compararea biometrică facială și validarea concordanțelor, în cazuri individuale și în condițiile legii. În partea ce ține de autorizarea judiciară prealabilă, aceasta nu poate fi instituită generic printr-o hotărâre de Guvern pentru orice utilizare a SI RIF. Regimul autorizării judiciare ține de legea

		Libertatea întrunirilor este garantată de art. 40 din Constituție și de art. 11 din CEDO. În cauza Gluhin împotriva Rusiei (2023), CtEDO a subliniat că utilizarea recunoașterii faciale în timp real impune cel mai înalt nivel de justificare și garanții specifice, cu atât mai necesare cu cât tehnologia permite identificarea fără ca persoana să fie în prealabil suspectă sau notificată. Propunere: Completarea cu o prevedere expresă care să stabilească restricții clare privind utilizarea SI RIF în contextul întrunirilor publice, cu indicarea cazurilor exhaustive în care identificarea biometrică în spații publice este permisă, cu condiția autorizării judiciare prealabile și a interdicției oricărei utilizări de natură să afecteze exercițiul dreptului garantat de art. 40 din Constituție și art. 11 din CEDO.	primară, în special de legislația procesual-penală și de actele normative speciale care reglementează măsurile restrictive de drepturi. Prin urmare, completarea propusă ar depăși obiectul proiectului și ar putea crea confuzie între SI RIF, ca sistem informațional de evidență și comparare a datelor de referință privind imaginile faciale, și sistemele de supraveghere video sau recunoaștere facială în timp real, care nu constituie obiectul de reglementare al prezentului proiect. Proiectul hotărârii de Guvern are caracter subsecvent și derivă din proiectul de lege privind cooperarea polițienească internațională (număr unic 264/MAI/2026), care constituie actul normativ de nivel superior în raport cu prezentul proiect
	24.	Regulamentul privind modalitatea de ținere a Registrului imaginilor faciale 4) Proprietarul fără obligații/controlul intern fără transparență Pct. 10 prevede „Proprietarul RIF este statul, care își realizează dreptul de proprietate, gestionare și utilizare a datelor din acesta, în condițiile legii.” Statul este declarat „proprietar”, dar nu are nicio secțiune dedicată drepturilor și obligațiile subiecților. Nici un singur drept sau obligație nu este atribuit explicit proprietarului. Entitățile care acționează în numele statului (MAI ca posesor) preiau toate atribuțiile, fără ca proprietarul să fie menționat ca subiect activ al unui raport juridic concret. Această prevedere creează un vid de responsabilitate incompatibil cu principiul legalității, echității și transparenței prevăzut la art. 5 lit. a) din alin.(1) la Legea nr. 195/2024. Se recomandă fie atribuirea unor obligații concrete proprietarului (în special privind supravegherea și răspunderea	**Se acceptă.** În redacția actuală a Regulamentului capitolul II a fost revizuit, urmare a avzelor recepționate. Totodată, în Concept au fost revizuite calitățile proprietarului și posesorului. Nu se consideră necesară instituirea unei secțiuni separate de drepturi și obligații pentru stat, întrucât statul, ca titular abstract al dreptului de proprietate publică, nu exercită nemijlocit operațiuni asupra datelor din RIF, acestea revenind autorităților și instituțiilor desemnate.

		față de persoanele vizate), fie eliminarea acestei calificări și reglementarea relației stat–MAI prin norme clare. b) La fel, este relevant și dreptul posesorului(MAI): „să aprobe regulile interne privind administrarea accesului, rolurile și profilurile de acces ale utilizatorilor” este incompatibil cu principiul transparenței impus de art. 5 alin. (1) lit. a) din Legea nr. 195/2024. c) Sintagma „mecanismele prevăzute de lege”, utilizată pentru notificarea actualizărilor bazei de date, nu identifică legea concretă, articolul aplicabil, destinatarul notificării sau termenul acesteia. Se propune indicarea expresă a Legii nr. 195/2024 și a CNPDCP ca destinatar obligatoriu al notificărilor.	
	25.	5) Dreptul deținătorului de a suspenda accesul fără procedură La pct. 25.3 este prevăzut dreptul deținătorului „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”. Deținătorul (organ tehnic subordonat MAI) poate suspenda accesul oricărei instituții fără criteriu obiectiv și fără termen limită al suspendării. Oficiul Avocatului Poporului consideră că această competență este formulată fără criterii obiective de activare, fără termen limită al suspendării, fără procedură de motivare și fără o cale de atac pentru instituțiile al căror acces a fost suspendat. Aceste revederi ar putea să intre în coliziune cu art. 20 din Constituție, care garantează dreptul oricărei persoane satisfacție efectivă, din partea instanțelor judecătorești competente împotriva actelor care violează drepturile, libertățile și interesele sale legitime. Propunere: Reformularea pct. 25 astfel încât să prevadă, o listă limitativă a situațiilor care justifică suspendarea, o durată	**Se acceptă.**

		maximă a suspendării cu posibilitate de prelungire motivată, obligația motivării în scris a deciziei de suspendare, o procedură de contestare în fața posesorului și, ulterior, a instanței de contencios administrativ.	
	26.	6) Contradicție internă și radiere a datelor biometrice fără garanții procedurale La pct. 30 există o contradicție, limitare a definiției de Registrator RIF. Avocatul Poporului consideră că există o contradicție între pct. 30 și pct. 15 din Regulament în privința definiției și competențelor registratorului RIF, incompatibilă cu cerința coerenței interne a actului normativ impusă de art. 53 alin. (1) din Legea nr. 100/2017. Se recomandă aducerea în concordanță textul celor două puncte pentru previzibilitate normativă. De asemenea, dreptul registratorilor de a „radia" date biometrice din RIF, prevăzut la pct. 30 lit. a), nu este însoțit de garanții procedurale. Potrivit art. 19 din Legea nr. 195/2024, Operatorul este obligat să comunice fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate. Propunere: Condiționarea radierii datelor biometrice din RIF de aprobarea scrisă a posesorului sau a unui superior ierarhic al registratorului.	**Se acceptă.** Punctele vizate au fost revizuite, iar motivele de radiere sunt prevăzute Capitolul IV Secțiunea 4 din Regulament
	27.	7) Competența discreționară nelimitată a MAI privind cerințele tehnice La pct. 23.1, posesorul (MAI) are dreptul de a stabili „cerințele funcționale, organizaționale și de securitate aplicabile RIF". Această competență este formulată fără nicio limită procedurală sau de fond nu se specifică dacă cerințele se aprobă prin ordin al ministrului, prin hotărâre de guvern sau prin act intern sau solicitarea unui aviz de la alte instituții. De menționat că potrivit art. 102 din Constituție, actele se emit în baza și în executarea legii, nu prin delegare discreționară nelimitată.	**Nu se acceptă.** Nu toate cerințele tehnice se aprobă prin ordinul ministrului afacerilor interne. O parte dintre aceste cerințe pot avea caracter tehnic, operațional sau de securitate și pot include informații privind arhitectura sistemului, profilurile de acces, mecanismele de securizare, jurnalizare, audit, configurare sau interoperabilitate. Astfel, publicarea tuturor cerințelor în Monitorul Oficial poate genera riscuri pentru securitatea sistemului.

		Propunere: Stabilirea în Regulament a obligației ca cerințele tehnice și de securitate ale SI RIF să fie aprobate prin ordin al ministrului afacerilor interne, publicat în Monitorul Oficial, cu avizul prealabil al CNPDCP și al Serviciului Tehnologia Informației și Securitate Cibernetică.	De asemenea, avizul prealabil obligatoriu al CNPDCP și al STISC pentru toate cerințele tehnice și de securitate ar fi excesiv. CNPDCP are competențe de supraveghere în domeniul protecției datelor, nu de avizare a cerințelor funcționale sau tehnice ale unui sistem informațional. STISC exercită atribuții de administrator tehnice al infrastructurii aferente găzduirii SI RIF.
	28.	8) Obligația de calitate a imaginilor nedefinită La pct. 35 este reglementată obligația furnizorului privind „calitatea suficientă a imaginilor". Calitate suficientă nu este definită în Regulament. Prin urmare, ar putea exista riscul ca furnizorul să nu poată ști cu certitudine dacă obligația sa este îndeplinită. Aceasta ar putea să contravină principiului limitării scopului și exactității conform art.5 lit.b) și d) din alin.(1) din Legea nr. 195/2024. Propunere: Definirea în Regulament a standardelor minime de calitate a imaginilor acceptate în RIF, cu referire la standarde tehnice verificabile aprobate.	**Se acceptă parțial.** Cerințele tehnice privind calitatea imaginilor, formatele, pragurile și regulile de comparare urmează a fi stabilite prin documentația tehnică a SI RIF, cu respectarea Regulamentului (UE) 2024/982, a Deciziei de punere în aplicare (UE) 2026/1064 și a standardelor europene și internaționale aplicabile. Totodată, în versiunea actualizată a proiectului, prevederile pct. 29 subpct. 2 și subpct. 8 din Regulament au fost revizuite.
	29.	9) Absența răspunderii diferențiate și a răspunderii statului față de persoana prejudiciată Capitolul III este intitulat „Drepturile și obligațiile subiecților la crearea, exploatarea și utilizarea RIF" însă nu există o secțiune de răspundere a subiecților. Din redacția actuală a proiecutlui nu pot fi identificate prevederi care să stabilească proceduri de controla, sau în general, mecanisme veritable de control și de răspundere în partea ce ține de activitatea privind crearea, exploatarea și utilizarea RIF. Art. 53 din Constituție, prevede dreptul persoanei vătămate de o autoritate publică la despăgubire. Art.76 din Legea nr. 195/2024 prevede dreptul de a obține despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.	**Precizare.** Răspunderea subiecților SI RIF și RIF este prevăzută la secțiunea 6 Capitolul VIII din Regulament.

		Propunere: Introducerea unei secțiuni distincte privind răspunderea diferențiată a fiecărui subiect raportat la atribuțiile sale, obligația statului/MAI de a despăgubi persoanele prejudiciate prin prelucrare neconformă, în termen determinat, procedura de sesizare și soluționare a cererilor de despăgubire.	
	30.	10) Scopul excesiv de larg al utilizării de către destinatari La pct. 37.2 este prevăzut dreptul destinatarilor de a „utiliza datele pentru identificarea persoanelor". Identificarea ori verificarea identității persoanelor este un scop extrem de larg, ar putea acoperi verificarea identității oricărei persoane în orice context, inclusiv în absența unui caz penal. Nu se impune existența unui caz individual, a unui ordin sau a unui mandat. Acesta ar putea să contravină art. 5 alin. (1) lit. b) din Legea nr. 195/2024, principiul limitării legate de scop. Propunere: Reformularea pct. 37.2 astfel încât utilizarea datelor pentru identificarea persoanei să fie condiționate motivat conform unui scop determinat.	**Se acceptă.** În varianta actuală, dreptul destinatarilor de a utiliza datele este la pct. 31 subpct. 2 din Regulament, care au fost revizuite conform obiecției înaintate.
	31.	11) Termene de stocare nedeterminate Secțiunea a 4-a din capitolul IV al Regulamentului (pct. 65-71) reglementează radierea, arhivarea și păstrarea datelor în RIF. Textul la pct. 71 prevede că datele se păstrează „numai pe perioada necesară realizării scopurilor pentru care au fost colectate", fără a defini în mod concret aceste termene. Avocatul Poporului consideră că această formulare este incompatibilă cu exigențele de previzibilitate ale normei juridice și cu principiul limitării stocării. Potrivit art. 5 alin. (1) lit. e) din Legea nr. 195/2024, datele cu caracter personal sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă ce nu depășește perioada necesară îndeplinirii scopurilor, principiu care impune operatorului să stabilească termene concrete nu generale.	**Se acceptă.** Secțiunea 4 din Capitolul IV a Regulamentului a fost revizuită.

		În contextul asigurării unui cadrul legal pertinent, este de remarcat că necesitatea unei reglementări corespunzătoare rezultă din constatările Studiului de evaluare a impactului digitalizării asupra drepturilor omului, elaborat și publicat cu suportul Institutului Danez pentru Drepturile Omului, potrivit căruia Republica Moldova nu dispune de un cadru normativ care să reglementeze utilizarea tehnologiilor de recunoaștere facială și a supravegherii biometrice în timp real în spațiile publice. Nu există norme explicite care să reglementeze stocarea, utilizarea și transferul transfrontalier al datelor biometrice. Acest vid normativ permite derularea programelor experimentale de supraveghere fără garanții privind necesitatea, proporționalitatea sau repararea individuală. În absența unor limite juridice clar definite și a unei supravegheri, există un risc înalt de încălcări ale vieții private și de monitorizare excesivă din partea statului. Propunere: Reglementarea unor termene maxime de stocare.	
	32.	12) Lista de mostre ca risc operațional La Secțiunea a 4-a din capitolul VI este reglementată lista mostrelor pentru care există posibilitatea unei concordanțe. La pct.126 Regulamentul definește „lista mostrelor pentru care există posibilitatea unei concordanțe” drept un „rezultat tehnic intermediar” al comparării automatizate. Deși textul declară că lista nu produce efecte de drept, în realitate ar putea exista riscul ca autoritățile operative de urmărire penală sau de frontieră, având acces vizual la o listă de potriviri biometrice probabile generată automat de algoritmul SI RIF, să folosească aceste informații „nevalidate” ca indicii suficiente pentru a dispune rețineri temporare, percheziții corporale sau interdicții de trecere a frontierei.	**Se acceptă.** Proiectul Regulamentului a fost completat cu prevederile de la pct. 130 și pct. 131.

		O asemenea practică ar putea să contravină cu art. 25 din Constituție care asigură respectarea libertății individuală și inviolabilitatea persoanei. Propunere: Introducerea unui punct nou în Regulament care să prevadă că Lista mostrelor pentru care există posibilitatea unei concordanțe nu poate fi utilizată, direct sau indirect, ca temei pentru dispunerea oricărei măsuri privative sau restrictive de drepturi, inclusiv reținere, percheziție corporală sau interdicție de traversare a frontierei.	
	33.	13) Absența obligației de notificare a CNPDCP în caz de incident Niciun subiect al RIF nu are obligația expresă de a sesiza Centrul Național pentru Protecția Datelor cu caracter Personal în caz de incident sau de prelucrare neconformă. Regulamentul se referă generic la „autoritățile competente” fără a le nominaliza. Potrivit art. 33 din Legea nr. 195/2024, operatorul are obligația de a notifica CNPDCP în termen de 72 de ore în caz de incident de securitate cu impact asupra datelor cu caracter personal. Iar potrivit art. 58 alin. (1) din Legea nr. 195/2024, Centrul asigură supravegherea și monitorizarea aplicării prezentei legi și a altor acte normative privind prelucrarea datelor cu caracter personal, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în legătură cu prelucrarea datelor cu caracter personal. Propunere: Introducerea unui punct nou în Regulament prin care Posesorul și deținătorul să fie obligat de a informa persoana vizată și de a notifica Centrul Național pentru Protecția Datelor cu Caracter Personal în termen de 72 de ore de la constatarea oricărui incident de securitate sau a oricărei prelucrări neconforme cu prezentul Regulament, cu transmiterea simultană a unui raport de incident și a planului de remediere.	**Se acceptă.**

Centrul Național Anticorupție (aviz nr. 06/2/11837 din 30.06.2026)	**34.**	În proiectul Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale (anexa nr. 2 la proiectul hotărârii de Guvern) – la punctul 16 de inclus Centrul Național Anticorupție în calitate de registrator; la punctul 21 de inclus Centrul Național Anticorupție în calitate de destinatar al datelor din SI Registrul imaginilor faciale. Includerea Centrului Național Anticorupție în calitate de registrator și destinatar al datelor din Sistemul Informațional Registrul imaginilor faciale este justificată prin competențele legale conferite instituției în domeniul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de corupție, a celor conexe, precum și a altor infracțiuni atribuite în competență. În exercitarea atribuțiilor sale, Centrul Național Anticorupție desfășoară activități speciale de investigații, activități de urmărire penală, expertize judiciare și alte măsuri procesuale care presupun identificarea și verificarea identității persoanelor vizate. Astfel, accesul la imaginile faciale și la datele asociate acestora reprezintă un instrument absolut necesar.	**Se acceptă.**
Centrul Național de Protecție a Datelor cu Caracter Personal (aviz nr. 04-01/2294 din 30.06.2026)	**35.**	Cu referire la proiectul hotărârii, se va nota că în preambulul/conținutul acesteia nu a fost identificat temeiul legal-legea specială care reglementează competența Ministerului Afacerilor Interne de a institui Sistemul informațional „Registrul imaginilor faciale” și de a colecta și prelucra imaginile faciale. Întrucât hotărârea este un act normativ subordonat legii, aceasta trebuie să se întemeieze în mod expres pe dispozițiile legale care conferă autorității publice competențele respective. Competența de a prelucra date cu caracter personal, în special categorii speciale de date nu poate fi instituită exclusiv printr-o hotărâre a Guvernului, ci trebuie să își aibă temeiul într-o lege adoptată de Parlament. O asemenea exigență decurge din	**Se acceptă parțial.** Preambulul și conținutul proiectului au fost revizuite în vederea indicării exprese a temeiurilor legale primare care permit instituirea SI RIF și prelucrarea imaginilor faciale, inclusiv prin raportare la cadrul normativ privind informatizarea și resursele informaționale de stat, registrele, protecția datelor cu caracter personal, activitatea autorităților competente și, după caz, legea specială privind cooperarea polițienească internațională. Se menționează că, proiectul de lege privind cooperarea polițienească internațională (număr unic 264/MAI/2026), care prezintă temeiul legal de

		principiul legalității ingerinței în dreptul la respectarea vieții private, consacrat de art. 8 alin. (2) din Convenția Europeană a Drepturilor Omului. Potrivit art. 8 alin. (2) din Convenție, orice ingerință a unei autorități publice în exercitarea dreptului la respectarea vieții private trebuie să fie „prevăzută de lege”, să urmărească unul sau mai multe scopuri legitime și să fie necesară într-o societate democratică. Sintagma „prevăzută de lege” nu se rezumă la existența formală a unui act normativ, ci presupune existența unei baze legale suficiente, accesibile și previzibile, care să definească în mod clar întinderea competențelor conferite autorităților publice și modalitatea de exercitare a acestora, oferind garanții adecvate împotriva arbitrariului. În aceste condiții, o hotărâre a Guvernului poate doar să detalieze modalitatea tehnică sau procedurală de punere în aplicare a unei competențe deja conferite prin lege, fără a crea ea însăși o nouă competență de prelucrare a datelor cu caracter personal. În caz contrar, executivul ar institui, printr-un act administrativ normativ, o ingerință în dreptul la viață privată, fără existența unei baze legale primare, ceea ce este incompatibil cu cerința ca ingerința să fie „prevăzută de lege” în sensul art. 8 din Convenție. Prin urmare, în măsura în care o hotărâre a Guvernului instituie pentru prima dată competența unei autorități de a colecta, utiliza, stoca, transmite sau prelucra date cu caracter personal, fără ca această competență să fie prevăzută de o lege, aceasta ridică serioase probleme de compatibilitate cu art. 8 din Convenția Europeană a Drepturilor Omului și cu principiul legalității ingerințelor în drepturile fundamentale.	instituire a Sistemului informațional „Registrul imaginilor faciale” a trecut etapele de avizare și expertizare, iar la moment conform criteriilor de referință parvenite de la Comisia Europeană, aceasta a fost expediată pentru consultare în adresa Comisiei, iar la etapa de parvenire a avizului Comisiei, aceasta va fi promovată în continuare conform procedurilor prevăzute de Legea nr. 100/2017 cu privire la actele normative. Este de menționat că, prezentul proiect de hotărâre după parcurgerea etapelor de avizare și expertizare, urmează a fi expediat în adresa Comisiei Europene pentru consultare, urmând a fi promovat ulterior conform procedurilor după etapa de adoptare a proiectului de Lege privind cooperarea polițienească internațională, care reprezintă actul legislativ superior. La fel, se menționează că prelucrarea datelor de referință privind imaginile faciale în scopul schimbului automatizat transfrontalier și operaționalizarea componentei aferente se va realiza numai după intrarea în vigoare a legii privind cooperarea polițienească internațională și în condițiile stabilite de aceasta, precum este prevăzut la pct. 5 (în versiunea revizuită) din hotărâre, care prevede că constituirea, utilizarea și punerea la dispoziție a setului de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier, precum și la funcționalitățile Sistemului informațional „Registrul imaginilor faciale” aferente schimbului automatizat transfrontalier se aplică de la data intrării în vigoare a Legii privind cooperarea polițienească

			internațională și în condițiile stabilite de aceasta, după îndeplinirea condițiilor juridice, organizatorice și tehnice necesare operaționalizării schimbului automatizat transfrontalier.
	36.	La pct. 19, subpct. 19.19. se exclude, întrucât 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 personala, este abrogată prin Hotărârea Guvernului nr. 678/2024 cu privire la modificarea și abrogarea unor hotărâri ale Guvernului (facilitarea activității mediului de afaceri VI). Totodată, cu titlu informativ, comunicăm că a fost instituită obligația operatorului de date cu caracter personal de a efectua evaluarea impactului asupra protecției datelor cu caracter personal, în cazul în care prelucrarea datelor poate genera un risc sporit pentru drepturile și libertățile persoanelor, precum și desemnarea unei persoane responsabile cu protecția datelor cu caracter personal (art. 23-25 din Legea nr. 133/2011 privind protecția datelor cu caracter personal). Astfel, ținând cont de prevederile art. 23 alin. (6) din Legea 133/2011, în cazul în care, tipurile de prelucrare a datelor cu caracter personal, reglementate prin actul normativ prenotat sunt susceptibile să genereze un risc sporit pentru drepturile și libertățile persoanelor, reieșind cel puțin din faptul prelucrării la scară largă a datelor cu caracter personal, este necesară efectuarea evaluării impactului asupra prelucrării datelor cu caracter personal, în contextul adoptării respectivului act normativ.	**Se acceptă.** Referința la Hotărârea Guvernului nr. 1123/2010 a fost exclusă din pct. 19 al Conceptului, iar prevederile privind evaluarea impactului asupra protecției datelor au fost revizuite la pct. 185 din Regulament.
Centrul de Armonizare a Legislației (aviz nr.	**37.**	În concluzie, clauza de armonizare a proiectului se va expune în următoarea redacție: „Prezenta Hotărâre pune în aplicare parțial art. 19 - 24 din Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024 privind căutarea și schimbul	**Se acceptă.** Cu referire la observația privind art. 23 din Regulamentul (UE) 2024/982, se ia act. Aspectele privind capacitățile maxime de căutare, procedura de majorare temporară sau permanentă și fluxul de

31/02-69-7670 din 30.06.2026)		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), CELEX: 32024R0982, publicat în Jurnalul Oficial al Uniunii Europene seria L 2024/982 din 5 aprilie 2024”.	notificare țin de etapa operaționalizării schimbului automatizat transfrontalier și vor fi asigurate în corelare cu legea privind căutarea și schimbul automatizat de date pentru cooperarea polițienească și cadrul normativ privind Punctul Unic de Contact și Punctele Naționale de Contact.
Serviciul Tehnologia Informațiilor și Securitate Cibernetică (aviz nr. 1.4/1223/26 din 30.06.2026)	**38.**	Reieșind din faptul că proiectul se poziționează ca actul care transpune parțial Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024 privind căutarea și schimbul automatizat de date în scopul cooperării polițienești, se constată că articolele 19–24 ale actului UE reglementează exclusiv mecanismul de schimb automatizat transfrontalier al datelor de referință privind imaginile faciale și limitează setul de date puse la dispoziție în acest scop la imaginile faciale ale suspecților, ale persoanelor condamnate și, după caz, ale victimelor. În același timp, proiectul propune constituirea și gestionarea unui Registru al imaginilor faciale cu un domeniu de aplicare semnificativ mai larg, care depășește categoriile de persoane și scopurile expres prevăzute de Regulamentul (UE) 2024/982. Or, nota informativă și proiectul nu conțin o justificare suficientă privind necesitatea, proporționalitatea și temeiul juridic al instituirii unei evidențe biometrice centralizate extinse, distincte de mecanismul de schimb transfrontalier reglementat de actul Uniunii Europene. Suplimentar, se relevă că imaginile faciale ale persoanelor sunt deja colectate și gestionate în cadrul Sistemului informațional „Registrul de stat al populației”, reglementat prin Hotărârea Guvernului nr. 236/2026, ceea ce impune argumentarea suplimentară a necesității constituirii unei resurse informaționale de stat distincte pentru stocarea și gestionarea imaginilor faciale.	**Se acceptă parțial.** Proiectul a fost revizuit în vederea delimitării clare dintre componenta națională a RIF și setul de date de referință privind imaginile faciale destinat schimbului automatizat transfrontalier. Se acceptă observația potrivit căreia art. 19–24 din Regulamentul (UE) 2024/982 reglementează mecanismul de căutare și schimb automatizat transfrontalier al datelor de referință privind imaginile faciale și nu instituirea, în sine, a unei evidențe biometrice naționale extinse. În acest sens, proiectul a fost precizat astfel încât setul de date de referință destinat schimbului automatizat transfrontalier să fie limitat la categoriile prevăzute de Regulamentul (UE) 2024/982 și de legea națională aplicabilă, cu excluderea datelor care permit identificarea directă a persoanei. Totodată, nu se acceptă observația în partea ce ține de limitarea întregului SI RIF exclusiv la categoriile de date necesare realizării obligațiilor ce decurg din Regulamentul (UE) 2024/982. SI RIF include o componentă națională distinctă, necesară pentru scopuri interne legitime, inclusiv prevenirea, constatarea și investigarea infracțiunilor, căutarea persoanelor dispărute, identificarea cadavrelor ori a părților acestora, gestionarea imaginilor faciale

		În aceste condiții, se consideră necesară revizuirea proiectului prin limitarea categoriilor de imagini faciale gestionate în cadrul sistemului la cele strict necesare pentru realizarea obligațiilor care decurg din Regulamentul (UE) 2024/982.	neidentificate, compararea biometrică facială, validarea concordanțelor, jurnalizarea, auditul și asigurarea trasabilității operațiunilor, în condițiile legii. Proiectul este elaborat în corelare cu proiectul de lege privind cooperarea polițienească internațională, nr. unic 264/MAI/2026, care urmează să constituie cadrul legal primar pentru componenta de schimb automatizat transfrontalier. Aplicarea prevederilor aferente schimbului automatizat transfrontalier al datelor de referință privind imaginile faciale va fi condiționată de intrarea în vigoare a legii speciale și de respectarea condițiilor juridice, organizatorice și tehnice prevăzute de aceasta. În ceea ce privește necesitatea unei resurse informaționale distincte față de Sistemul informațional „Registrul de stat al populației”, Nota de fundamentare a fost completată pentru a evidenția finalitatea diferită a SI RIF. Registrul de stat al populației are o finalitate distinctă, orientată spre evidența populației și documentarea persoanelor, în timp ce SI RIF are o destinație specializată, orientată spre gestionarea imaginilor faciale și a datelor de referință în scopuri polițienești, criminalistice, de căutare, validare biometrică, jurnalizare, audit, trasabilitate și cooperare polițienească internațională. În contextul observațiilor privind prelucrarea datelor biometrice ale victimelor, pct. 10.3 din Concept și pct. 50-51 din Regulament au fost revizuite astfel încât să rezulte expres că datele de referință privind imaginile faciale ale victimelor pot fi incluse în setul de date destinat schimbului

			automatizat transfrontalier numai în cazurile, condițiile și limitele prevăzute expres de lege, cu respectarea principiilor legalității, necesității, proporționalității, limitării scopului, minimizării datelor și protecției datelor cu caracter personal.
	39.	Referitor la proiectul de hotărâre: 1. Se va reformula pct. 4 din proiectul hotărârii, astfel încât să fie stabilit în mod clar momentul aplicării prevederilor respective. Redacția actuală poate crea incertitudini privind data de la care normele devin aplicabile, contrar principiilor clarității și predictibilității prevăzute la art. 3 din Legea nr. 100/2017 cu privire la actele normative;	**Se acceptă.** În versiunea revizuită pct. 5 din hotărâre.
	40.	Cu referire la proiectul Conceptului: 2. La pct. 19, subpct. 19.19, se va exclude 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, ținând cont de faptul că aceasta a fost abrogată;	**Se acceptă.**
	41.	3. Pct. 36, se va ajusta ținând cont de prevederile art. 7 alin. (2) din Legea nr. 467-XV/2003 cu privire la informatizare și la resursele informaționale de stat, conform cărora: „(2) Subiecţi ai raporturilor juridice în domeniul creării, administrării, mentenanţei, dezvoltării şi utilizării sistemelor informaţionale de stat sunt: a) proprietarul sistemului informaţional; b) posesorul sistemului informaţional; c) deţinătorul sistemului informaţional; d) administratorul tehnic al sistemului informaţional; e) utilizatorii sistemului informaţional.”;	**Se acceptă.**
	42.	4. La pct. 39, se va exclude textul “și în coordonare cu administratorul tehnic pentru aspectele ce țin de găzduire și infrastructura tehnologiilor informaționale”, deoarece păstrarea acestuia este inoportună, având în vedere faptul că atribuțiile administratorului tehnic sunt deja prevăzute în Regulamentul privind administrarea tehnică și menținerea resurselor și	**Se acceptă.**

		sistemelor informaționale de stat aprobat prin Anexa nr. 5 la Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaționale de stat;	
	43.	5. Pct. 40, se va expune astfel: "Administratorul tehnic al SI RIF este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică", care asigură administrarea tehnică în conformitate cu Anexa nr. 5 aprobată prin Hotărârea Guvernului 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat";	**Se acceptă.**
	44.	6. Pct. 74, va avea următorul cuprins: "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) și este compatibil cu platforma de găzduire bazată pe tehnologii de tip container, care presupune utilizarea rațională a resurselor.";	**Se acceptă.**
	45.	7. Prevederea de la pct. 108, se va exclude, ținând cont că găzduirea SI RIF se realizează în conformitate cu prevederile pct. 74 în redacția expusă supra;	**Se acceptă.**
	46.	8. La pct. 118 se va exclude textul "și administratorul tehnic", având în vedere că atribuțiile administratorului tehnic sunt deja reglementate de cadrul normativ în materie de administrare tehnică și menținere a resurselor și sistemelor informaționale de stat;	**Se acceptă.**
	47.	Cu referire la proiectul Regulamentului: 9. Pct. 9 se va ajusta în conformitate cu prevederile art. 9 din Legea nr. 71-XVI/2007 cu privire la registre, conform cărora: „Subiecţi ai raporturilor juridice în domeniul registrelor sînt: a) proprietarul registrului; b) posesorul registrului; c) deţinătorul registrului; d) registratorul și subregistratorul; e) furnizorul datelor registrului; f) destinatarul datelor registrului.";	**Se acceptă.**

	48.	10. Din cuprinsul proiectului Regulamentului, se va exclude administratorul tehnic, fiind un subiect al raporturilor juridice în domeniul creării, administrării, mentenanţei, dezvoltării şi utilizării sistemelor informaţionale de stat care se regăsește deja în Conceptul SI RIF. Prevederile ce țin de administrarea tehnică, securitatea Sistemului și protecția informației, se vor regăsi în Conceptul acestuia, în conformitate cu art. 76, alin. (2), lit. a) din Legea nr. 467/2003.	**Se acceptă.**
	49.	11. Pct. 188, se va exclude, întrucât, conform Hotărârii Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud), pe platformă sunt găzduite sistemele informaționale, și nu resurse informaționale. Mai mult, prevederile privind găzduirea SI RIF sunt deja reglementate în proiectul de Concept;	**Se acceptă.**
	50.	Referitor la Nota de Fundamentare: 12. La compartimentele 3, 4 și 9, prevederile ce țin de administratorul tehnic se vor reformula corespunzător cu obiecțiile expuse în Concept;	**Se acceptă.**
	51.	13. La compartimentul 3, subpct. 3.1., la alin. 13 sintagma “platforma MCloud” se va exclude, deoarece SI RIF nu utilizează această platformă, ci este găzduit pe platforma tehnologică guvernamentală comună (MCloud);	**Se acceptă.**
	52.	14. La compartimentul 4, subpct. 4.2., Impactul financiar și argumentarea costurilor estimative, se va completa cu următorul alineat: „Urmare a dării în exploatare a SI RIF, Posesorul va încheia cu Administratorul tehnic, Acordul privind administrarea tehnică și menținerea SI RIF, care va include activitățile minime privind administrarea tehnică și menținerea RIF, precum și volumul acestora. În baza Acordului vor fi estimate cheltuielile pentru administrare tehnică a SI RIF care urmează a fi acoperite din bugetul de stat, prin intermediul granturilor oferite Instituției Publice „Serviciul Tehnologia Informației și Securitate Cibernetică”, de către fondator.”.	**Se acceptă.**

	53.	15. Se constată că proiectul este promovat exclusiv în scopul implementării parțiale a Regulamentului (UE) 2024/982, iar potrivit tabelului de concordanță și notei informative, celelalte dispoziții relevante ale actului european urmează să fie transpuse prin proiectul de lege privind cooperarea polițienească internațională, aflat încă în proces de examinare și aprobare. În acest context, se relevă că proiectul supus avizării instituie elemente esențiale ale Sistemului informațional „Registrul imaginilor faciale", inclusiv scopul, obiectele informaționale, categoriile de date prelucrate, mecanismele de schimb automatizat și rolurile instituționale, în lipsa unei baze legale primare definitive care să reglementeze expres aceste aspecte. Or, având în vedere că proiectul de lege privind cooperarea polițienească internațională nu este adoptat și poate suferi modificări semnificative pe parcursul procedurii legislative, nu există certitudinea că soluțiile normative prevăzute în proiectul hotărârii de Guvern vor corespunde formei finale a cadrului legal primar. În consecință, există riscul ca, ulterior adoptării legii, prezentul proiect să necesite revizuiri substanțiale pentru a fi aliniat prevederilor legale adoptate de Parlament. Prin urmare, se consideră prematură promovarea și aprobarea proiectului în forma propusă până la adoptarea și intrarea în vigoare a proiectului de lege privind cooperarea polițienească internațională, astfel încât soluțiile instituționale și tehnice prevăzute de prezentul proiect să poată fi evaluate și ajustate în raport cu forma finală a cadrului legal primar. În lipsa adoptării cadrului legal primar, proiectul operează cu concepte, proceduri și mecanisme juridice care încă nu au fost consacrate de legiuitor (schimb automatizat transfrontalier de imagini faciale, puncte de contact naționale, numere de referință, confirmarea concordanțelor, schimbul de informații	**Se acceptă parțial.** Se menționează că, proiectul de lege privind cooperarea polițienească internațională (număr unic 264/MAI/2026), care prezintă temeiul legal de instituire a Sistemului informațional „Registrul imaginilor faciale" a trecut etapele de avizare și expertizare, iar la moment conform criteriilor de referință parvenite de la Comisia Europeană, aceasta a fost expediată pentru consultare în adresa Comisiei, iar la etapa de parvenire a avizului Comisiei, aceasta va fi promovată în continuare conform procedurilor prevăzute de Legea nr. 100/2017 cu privire la actele normative. Este de menționat că, prezentul proiect de hotărâre după parcurgerea etapelor de avizare și expertizare, urmează a fi expediat în adresa Comisiei Europene pentru consultare, urmând a fi promovat ulterior conform procedurilor după etapa de adoptare a proiectului de Lege privind cooperarea polițienească internațională, care reprezintă actul legislativ superior. La fel, se menționează că prelucrarea datelor de referință privind imaginile faciale în scopul schimbului automatizat transfrontalier și operaționalizarea componentei aferente se va realiza numai după intrarea în vigoare a legii privind cooperarea polițienească internațională și în condițiile stabilite de aceasta, precum este prevăzut la pct. 5 din hotărâre (versiunea revizuită), care prevede că constituirea, utilizarea și punerea la dispoziție a setului de date de referință privind imaginile faciale destinat schimbul automatizat transfrontalier, precum și la funcționalitățile

		ulterior concordanței etc.), ceea ce poate conduce la aprobarea unui act normativ a Guvernului bazat pe soluții legislative nevalidate de Parlament.	Sistemului informațional „Registrul imaginilor faciale" aferente schimbului automatizat transfrontalier se aplică de la data intrării în vigoare a Legii privind cooperarea polițienească internațională și în condițiile stabilite de aceasta, după îndeplinirea condițiilor juridice, organizatorice și tehnice necesare operaționalizării schimbului automatizat transfrontalier.
Ministerul Muncii și Protecției Sociale (aviz nr. nr.22/3558 din 30.06.2026	**54.**	Comunică lipsa obiecțiilor și propunerilor	**S-a luat act.**
Ministerul Justiției (aviz nr.04/1-7394 din 03.07.2026)	**55.**	Obiecții la proiectul hotărârii: Clauza de armonizare se va revizui și se va aduce în concordanță cu prevederile pct. 37 din Regulamentul privind armonizarea legislației Republicii Moldova cu legislația UE, aprobat prin Hotărârea Guvernului nr. 1171/2018, dat fiind că este indicat atât faptul că transpune parțial Regulamentul (UE) 2024/982, cât și ce articole transpune.	**Se acceptă.** Clauza de armonizare a fost revizuită în conformitate cu propunerile parvenite din partea Centrului de Armonizare a Legislației.
	56.	Obiecții la proiectul conceptului: Parafa de aprobare a anexei se va indica după cum urmează: „Anexa nr. 1 la Hotărârea Guvernului nr. ____/2026". Obiecție valabilă și la anexa nr. 2.	**Se acceptă.**
	57.	Referitor la cuprinsul pct. 15 recomandăm revizuirea acestuia, deoarece unele principii care necesită a fi respectate la proiectarea, dezvoltarea și implementarea SI RIF nu corespund noţiunii de principiu, or, nu toate regulile de organizare şi funcţionare a sistemului informaţional trebuie ridicate la nivel de principiu.	**Se acceptă.**
	58.	La pct. 19 se evidențiază faptul că lista actelor normative indicate, deși este una extinsă, nu cuprinde referințe la cadrul	**Se acceptă.**

		normativ execuțional-penal. În acest context, se remarcă lipsa trimiterilor la Codul de executare nr. 443/2004 (art. 202 alin. (2)), Legea nr. 300/2017 cu privire la sistemul administrației penitenciare (art. 13 alin. (2) lit. i)), Hotărârea Guvernului nr. 716/2014 pentru aprobarea Regulamentului cu privire la Registrul persoanelor reținute, arestate și condamnate, acte normative care reglementează regimul juridic al persoanelor private de libertate. Această omisiune prezintă relevanță în condițiile în care, potrivit subpct. 19.6 și 21.6 din Regulament, Administrația Națională a Penitenciarelor este desemnată atât în calitate de furnizor, cât și de destinatar de date în cadrul SI RIF, iar potrivit subpct. 10.3 din Concept, printre categoriile de persoane ale căror imagini faciale pot fi incluse în setul de date destinat schimbului transfrontalier se regăsesc și persoanele condamnate. Astfel, deși proiectul instituie un cadru detaliat privind prelucrarea imaginilor faciale de către autoritățile competente, raportarea acestui mecanism la regimul juridic aplicabil executării pedepselor privative de libertate rămâne insuficient clarificată. Prin urmare, în vederea asigurării unei corelări corespunzătoare între regimul de prelucrare a datelor biometrice și cadrul normativ specific domeniului execuțional penal, se apreciază oportună completarea pct. 19 din Concept cu referințe exprese la Codul de executare nr. 443/2004, la Legea nr. 300/2017 cu privire la sistemul administrației penitenciare și Hotărârea Guvernului nr. 417/2014 pentru aprobarea Regulamentului cu privire la Registrul persoanelor reținute, arestate și condamnate.	
	59.	La pct. 39 cuvintele „Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne” se va substitui cu cuvintele „Serviciul Tehnologii Informaționale din subordinea	**Se acceptă.**

		Ministerului Afacerilor Interne”, în conformitate cu pct. 2 din Regulamentul privind organizarea și funcționarea Serviciului Tehnologii Informaționale, aprobat prin Hotărârea Guvernului nr. 317/2020. Obiecția dată este valabilă și pentru pct. 12 și 25 din anexa nr. 2.	
	60.	Potrivit prevederilor proiectului, validarea concordanței stabilite în urma comparării automatizate efectuate prin intermediul SI RIF are caracter consultativ și nu substituie verificările și actele procedurale prevăzute de legislația Republicii Moldova. În aceste condiții, participarea aceleiași persoane atât la validarea concordanței rezultatului comparării automatizate, cât și, ulterior, în calitate de specialist sau expert judiciar, la verificarea ori evaluarea aceluiași rezultat în cadrul unei cauze, ar determina cumularea unor atribuții susceptibile să afecteze obiectivitatea și imparțialitatea examinării. Persoana respectivă ar fi pusă, în esență, în situația de a verifica, confirma sau aprecia, într-o calitate procesuală, rezultatul la formarea ori validarea căruia a participat anterior. Necesitatea reglementării exprese a acestei incompatibilități rezultă din art. 87 alin. (9) din Codul de procedură penală, potrivit căruia recuzarea specialistului se efectuează în condițiile prevăzute pentru recuzarea interpretului și traducătorului, prin aplicarea corespunzătoare a prevederilor art. 33 din același cod. Totodată, art. 89 alin. (1) pct. 4) din Codul de procedură penală prevede recuzarea expertului în cazul în care acesta a efectuat, în cauza respectivă, o revizie sau alte acțiuni de control ale căror rezultate au servit drept temei pentru pornirea procesului penal. Deși validarea concordanței efectuată în cadrul SI RIF nu poate fi asimilată în toate cazurile unei revizii sau unei acțiuni de control în sensul strict al normei menționate, rațiunea acestei incompatibilități este aplicabilă și situației examinate: separarea persoanei care a participat la obținerea ori	**Se acceptă parțial.** Regulamentul a fost completat la pct. 137 cu o prevedere privind incompatibilitatea persoanei care a participat la validarea concordanței rezultate din compararea automatizată efectuată prin SI RIF de a participa ulterior, în aceeași cauză, în calitate de specialist sau expert judiciar, la examinarea, verificarea ori evaluarea aceluiași rezultat sau a aceleiași concordanțe. Textul propus de Ministerul Justiției a fost ajustat pentru a limita incompatibilitatea la aceeași cauză și la același rezultat al comparării automatizate, evitând instituirea unei interdicții generale și nediferențiate pentru orice expertiză sau act procedural.

		validarea rezultatului preliminar de persoana care urmează să îl examineze și să îl aprecieze ulterior într-o calitate procesuală. Lipsa unei asemenea delimitări poate genera îndoieli rezonabile privind imparțialitatea specialistului sau a expertului judiciar, poate determina formularea unor cereri de recuzare și poate afecta admisibilitatea, credibilitatea ori forța probantă a rezultatelor obținute în cadrul procedurii. O soluție normativă similară este prevăzută în Regulamentul privind modalitatea de ținere a Registrului de stat al datelor genetice, aprobat prin Hotărârea Guvernului nr. 821/2023, care stabilește pentru personalul implicat în activitatea registrului obligația de a nu efectua, în perioada exercitării funcției, cercetări sau expertize judiciare în specialitatea „expertiza genetică” (art. 17, pct. 13 din Anexa nr. 2). Această interdicție urmărește separarea funcțională dintre activitatea de gestionare și validare a datelor din registru și activitatea de examinare a acestora în cadrul unei expertize judiciare. Prin urmare, pentru asigurarea imparțialității, evitarea cumulării unor atribuții incompatibile și prevenirea eventualelor incidente procesuale privind recuzarea specialistului sau a expertului judiciar, se propune completarea capitolului V, secțiunii a 5-a din proiectul Regulamentului privind modalitatea de ținere a Registrului imaginilor faciale cu un punct cu următorul cuprins: „Personalul calificat, care a participat la validarea concordanței a rezultatului comparării automatizate SI RIF, nu poate participa ulterior la expertize sau acte procedurale cerute de lege în calitate de „specialist” sau „expert judiciar”.”.	
Agenția de Guvernare Electronică (aviz	**61.**	Comunică lipsa obiecțiilor și propunerilor.	**S-a luat act.**

nr. 3007 – 215 din 06.07.2026)			
Serviciul de Informații și Securitate (aviz nr. IE/6767 din 07.07.2026)	**62.**	Comunică lipsa obiecțiilor și propunerilor.	**S-a luat act.**
Procedura de expertizare			
Centrul Național Anticorupție (expertiza anticorupție nr. EHG26/11723 din 27.07.2026)	**63.**	În final, menționăm că proiectul promovează interesul public manifestat prin instituirea Sistemului informațional „Registrul imaginilor faciale” în vederea racordării cadrului legal la normele comunitare în domeniu. Totodată, menționăm că prezentul raport de expertiză anticorupție nu se răsfrânge asupra normelor din proiect ce se referă la proiectul Conceptului Sistemului informațional „Registrul imaginilor faciale” (anexa nr. 1 din proiectul hotărârii de Guvern), din considerentul că acesta este exceptat de la realizarea expertizei anticorupție potrivit prevederilor art. 28 alin. (2) lit. a) și g) din Legea integrității nr. 82/2017, corelat cu art. 36 din Legea nr. 100/2017 cu privire la actele normative.	**S-a luat act.**
Ministerul Justiției (expertiza juridică nr. 04/1-8797 din 03.08.2026)	**64.**	Comunicăm că observațiile formulate de către Ministerul Justiției în avizul nr. 04/1-7394 din 03.07.2026, au fost luate în considerare, proiectul fiind revizuit prin prisma acestora. La forma actuală a proiectului, se reţin următoarele: Obiecții la proiectul Conceptului: La pct. 12 noțiunile se vor expune în ordine alfabetică.	**Se acceptă.**
	65.	La pct. 17 textul „ , aprobat prin prezenta hotărâre” nu este necesar și se va exclude.	**Se acceptă.**
	66.	La pct. 18 referitor la referința la actele Uniunii Europene, se va ține cont că deşi legislația Uniunii Europene (directive/regulamente) sunt instrumente juridice de importanţă	**Se acceptă.**

		majoră la nivelul Uniunii Europene, pentru Republica Moldova nu sunt direct aplicabile. Legislația Uniunii Europene urmează să fie transpusă în legislaţia naţională (obiecție valabilă și la pct. 20 și 113).	
	67.	La pct. 19 actele normative se vor indica în ordine cronologică cu respectarea ierarhiei.	**Se acceptă.**
	68.	La sbp. 19.39 se va ține cont că, potrivit art. 11 alin. (1) lit. k) din Legea nr. 98/2012 privind administrația publică centrală de specialitate, ministrul emite în mod unipersonal ordine în limitele competenţei sale, dar nu ministerul.	**Se acceptă.**
	69.	La pct. 40 textul „Anexa nr. 5 la” se va exclude.	**Se acceptă.**
	70.	La pct. 80 se va revizui referința la pct. 76, deoarece nu este corectă.	**Se acceptă.**
	71.	La pct. 122 se va indica denumirea completă a actului normativ.	**Se acceptă.**
	72.	Obiecții la proiectul regulamentului: Cuprinsul pct. 7 ține de obiectul de reglementare a capitolului IV, secțiunea 1. Astfel, pentru a nu dubla prevederile, la pct. 33 se va indica și limba în care se ține RIF.	**Se acceptă.** Prevederile pct. 7 din Regulament au fost revizuite.
	73.	La pct. 206 pentru claritate, se va indica exact cuprinsul art. 33 alin. (1) din Legea nr. 195/2024 privind protecția datelor cu caracter personal sau se va face trimitere la articolul menționat.	**Se acceptă.**