# 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)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16 alineatul (2), articolul 87 alineatul (2) litera (a) și articolul 88 alineatul (2),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European ([1]),

hotărând în conformitate cu procedura legislativă ordinară ([2]),

întrucât:

(1) Uniunea și-a stabilit obiectivul de a le oferi cetățenilor săi un spațiu de libertate, securitate și justiție fără frontiere interne, în interiorul căruia este asigurată libera circulație a persoanelor. Obiectivul respectiv trebuie să fie realizat, printre altele, prin intermediul unor măsuri adecvate de prevenire și combatere a criminalității și a altor amenințări la adresa securității publice, inclusiv a criminalității organizate și a terorismului, în conformitate cu Comunicarea Comisiei din 24 iulie 2020 referitoare la Strategia UE privind uniunea securității. Respectivul obiectiv impune ca autoritățile de aplicare a legii să facă schimb de date, în mod eficient și în timp util, pentru a preveni, a detecta și a investiga în mod eficace infracțiunile.

(2) Obiectivul prezentului regulament este de a îmbunătăți, raționaliza și facilita, în scopul prevenirii, depistării și investigării infracțiunilor, schimbul de informații în materie penală și referitoare la datele de înmatriculare ale vehiculelor între autoritățile competente din statele membre și între statele membre și Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol), instituită prin Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului ([3]), cu respectarea deplină a drepturilor fundamentale și a normelor privind protecția datelor.

(3) Deciziile 2008/615/JAI ([4]) și 2008/616/JAI ([5]) ale Consiliului, care stabilesc normele pentru schimbul de informații între autoritățile cu atribuții de prevenire și investigare a infracțiunilor prin asigurarea transferului automatizat de profiluri ADN, de date dactiloscopice și de anumite date privind înmatricularea vehiculelor s-au dovedit importante pentru combaterea terorismului și a criminalității transfrontaliere, protejând astfel securitatea internă a Uniunii și a cetățenilor săi.

(4) Pe baza procedurilor existente pentru căutarea automatizată a datelor, prezentul regulament stabilește condițiile și procedurile pentru căutarea și schimbul automatizat de profiluri ADN, date dactiloscopice, anumite date privind înmatricularea vehiculelor, imagini faciale și evidențe ale poliției. Acest lucru nu ar trebui să aducă atingere

([1]) JO C 323, 26.8.2022, p. 69.
([2]) Poziția Parlamentului European din 8 februarie 2024 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 26 februarie 2024.
([3]) Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului (JO L 135, 24.5.2016, p. 53).
([4]) Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008, p. 1).
([5]) Decizia 2008/616/JAI a Consiliului din 23 iunie 2008 privind punerea în aplicare a Deciziei 2008/615/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008, p. 12).

prelucrării de astfel de date în Sistemul de Informații Schengen (SIS), schimbului de informații suplimentare referitoare la astfel de date prin intermediul birourilor SIRENE în temeiul Regulamentului (UE) 2018/1862 al Parlamentului European și al Consiliului ([6]) sau drepturilor persoanelor ale căror date sunt prelucrate în cadrul acestora.

(5) Prezentul regulament stabilește un cadru pentru schimbul de informații între autoritățile responsabile cu prevenirea, depistarea și investigarea infracțiunilor (denumit în continuare „cadrul Prüm II"). În conformitate cu articolul 87 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE), acesta vizează toate autoritățile competente ale statelor membre, inclusiv dar nelimitat la poliție, serviciile vamale și alte servicii de aplicare a legii specializate în prevenirea, depistarea și investigarea infracțiunilor. Prin urmare, în contextul prezentului regulament, orice autoritate care este responsabilă de gestionarea unei baze de date naționale care intră sub incidența prezentului regulament sau care acordă o autorizație judiciară de divulgare a oricăror date ar trebui considerată ca intrând în domeniul de aplicare al prezentului regulament, atât timp cât informațiile sunt schimbate pentru prevenirea, depistarea și investigarea infracțiunilor.

(6) Nicio acțiune de prelucrare de date cu caracter personal sau schimb de date cu caracter personal în sensul prezentului regulament nu ar trebui să conducă la discriminarea persoanelor din niciun motiv. Aceste acțiuni ar trebui să respecte pe deplin demnitatea și integritatea umană și celelalte drepturi fundamentale, inclusiv dreptul la respectarea vieții private și la protecția datelor cu caracter personal, în conformitate cu Carta drepturilor fundamentale a Uniunii Europene.

(7) Orice prelucrare sau schimb de date cu caracter personal ar trebui să facă obiectul dispozițiilor referitoare la protecția datelor cuprinse în capitolul 6 din prezentul regulament și, după caz, al dispozițiilor Directivei (UE) 2016/680 a Parlamentului European și a Consiliului ([7]), ale Regulamentului (UE) 2018/1725 al Parlamentului European și al Consiliului ([8]), ale Regulamentului (UE) 2016/794 sau ale Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului ([9]). Directiva (UE) 2016/680 se aplică utilizării cadrului Prüm II în ceea ce privește căutările persoanelor dispărute și identificarea rămășițelor umane neidentificate în scopul prevenirii, depistării și investigării infracțiunilor, în timp ce Regulamentul (UE) 2016/679 se aplică utilizării cadrului Prüm II în ceea ce privește căutarea persoanelor dispărute și identificarea rămășițelor umane neidentificate în alte scopuri.

(8) Deoarece prevede căutarea automatizată a profilurilor ADN, a datelor dactiloscopice, a anumitor date privind înmatricularea vehiculelor, a imaginilor faciale și a evidențelor poliției, scopul prezentului regulament este, de asemenea, de a facilita căutarea persoanelor dispărute și identificarea rămășițelor umane neidentificate. Respectivele căutări automatizate ar trebui să respecte normele și procedurile prevăzute în prezentul regulament. Respectivele căutări automatizate nu aduc atingere introducerii semnalărilor cu privire la persoane dispărute în SIS și schimbului de informații suplimentare cu privire la astfel de semnalări în temeiul Regulamentului (UE) 2018/1862.

(9) În cazul în care statele membre doresc să utilizeze cadrul Prüm II pentru a căuta persoane dispărute și pentru a identifica rămășițe umane, acestea ar trebui să adopte măsuri legislative naționale pentru a desemna autoritățile naționale competente în acest scop pentru a stabili procedurile, condițiile și criteriile specifice în acest sens. În cazul căutării de persoane dispărute în afara domeniului anchetelor penale, măsurile legislative naționale ar trebui să

([6]) Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală, de modificare și de abrogare a Deciziei 2007/533/JAI a Consiliului și de abrogare a Regulamentului (CE) nr. 1986/2006 al Parlamentului European și al Consiliului și a Deciziei 2010/261/UE a Comisiei (JO L 312, 7.12.2018, p. 56).

([7]) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

([8]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

([9]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

stabilească în mod clar motivele umanitare în temeiul cărora se poate efectua căutarea persoanelor dispărute. Astfel de căutări ar trebui să respecte principiul proporționalității. Motivele umanitare ar trebui să includă situații de dezastre naturale și provocate de om și alte motive la fel de justificate, cum ar fi suspiciunile de sinucidere.

(10) Prezentul regulament prevede condițiile și procedurile pentru căutarea automatizată de profiluri ADN, de date dactiloscopice, de anumite date privind înmatricularea vehiculelor, de imagini faciale și de evidențe ale poliției, precum și normele privind schimbul de date de bază în urma unei concordanțe confirmate privind datele biometrice. Acesta nu se aplică schimbului de informații suplimentare în afara celor prevăzute în prezentul regulament, care este reglementat prin Directiva (UE) 2023/977 a Parlamentului European și a Consiliului ([10]).

(11) Directiva (UE) 2023/977 oferă un cadru juridic coerent al Uniunii prin care se va asigura faptul că autoritățile competente ale unui stat membru au acces echivalent la informațiile deținute de alte state membre atunci când au nevoie de astfel de informații pentru a combate criminalitatea și terorismul. Pentru a consolida schimbul de informații, directiva formalizează și clarifică normele și procedurile pentru schimburile de informații între autoritățile competente ale statelor membre, în special în scopul desfășurării anchetelor, inclusiv rolul punctului unic de contact al fiecărui stat membru în astfel de schimburi.

(12) Scopul schimburilor de profiluri ADN în temeiul prezentului regulament nu aduce atingere competenței exclusive a statelor membre de a decide scopul bazelor lor de date ADN naționale, inclusiv în scopuri de prevenire sau depistare a infracțiunilor.

(13) Statele membre ar trebui ca la momentul conectării inițiale la router stabilit prin prezentul regulament, să efectueze căutări automatizate ale profilurilor ADN prin compararea tuturor profilurilor ADN stocate în bazele lor de date cu toate profilurile ADN stocate în bazele de date ale tuturor celorlalte state membre și cu datele Europol. Scopul respectivei căutări automatizate inițiale este de a evita orice lacune în identificarea concordanțelor între profilurile ADN stocate în baza de date a unui stat membru și profilurile ADN stocate în bazele de date ale tuturor celorlalte state membre și în datele Europol. Căutarea automatizată inițială ar trebui realizată la nivel bilateral și nu ar trebui efectuată neapărat în același timp cu bazele de date ale tuturor celorlalte statele membre și cu datele Europol. Măsurile pentru efectuarea unor astfel de căutări, inclusiv calendarul și cantitatea pe loturi, ar trebui convenite bilateral în conformitate cu normele și procedurile prevăzute în prezentul regulament.

(14) În urma căutării automatizate a profilurilor ADN, statele membre ar trebui să efectueze căutări automatizate prin compararea tuturor profilurilor ADN nou adăugate în bazele lor de date cu toate profilurile ADN stocate în bazele de date ale altor state membre și cu datele Europol. Respectiva căutare automatizată a noilor profiluri ADN ar trebui să aibă loc în mod regulat. În cazul în care astfel de căutări nu ar putea avea loc, statul membru în cauză ar trebui să aibă posibilitatea de a le efectua într-o etapă ulterioară, pentru a se asigura că nu au fost omise concordanțe. Modalitățile de efectuare a unor astfel de căutări ulterioare, inclusiv calendarul și cantitatea pe loturi, ar trebui convenite la nivel bilateral în conformitate cu normele și procedurile prevăzute în prezentul regulament.

(15) Pentru căutarea automatizată a anumitor date privind înmatricularea vehiculelor, statele membre și Europol ar trebui să utilizeze Sistemul de informații european privind vehiculele și permisele de conducere (Eucaris), instituit prin Tratatul privind Sistemul european de informații privind vehiculele și permisele de conducere (EUCARIS) și care este conceput în acest scop, care conectează toate statele membre participante la o rețea. Nu este necesară o componentă centrală pentru stabilirea comunicării, întrucât fiecare stat membru comunică direct cu celelalte state membre conectate, iar Europol comunică direct cu bazele de date conectate.

(16) Identificarea unui infractor este esențială pentru succesul investigației și urmăririi penale. Căutarea automatizată a imaginilor faciale ale persoanelor condamnate sau suspectate de a fi comis o infracțiune, sau, în cazul în care dreptul intern al statului membru solicitat permite acest lucru, imaginile faciale ale victimelor, colectate în conformitate cu dreptul intern, ar putea să ofere informații suplimentare pentru identificarea cu succes a

([10]) Directiva (UE) 2023/977 a Parlamentului European și a Consiliului din 10 mai 2023 privind schimbul de informații dintre autoritățile de aplicare a legii ale statelor membre și de abrogare a Deciziei-cadru 2006/960/JAI a Consiliului (JO L 134, 22.5.2023, p. 1).

infractorilor și pentru combaterea criminalității. Având în vedere caracterul sensibil al datelor în cauză, ar trebui să fie posibilă efectuarea de căutări automatizate numai în scopul prevenirii, depistării sau investigării unei infracțiuni pasibile de o pedeapsă maximă cu închisoarea de cel puțin un an în temeiul legislației statului membru solicitant.

(17) Căutarea automatizată a datelor biometrice de către autoritățile competente ale statelor membre, responsabile cu prevenirea, depistarea și investigarea infracțiunilor în temeiul prezentului regulament ar trebui să vizeze numai datele conținute în bazele de date create pentru prevenirea, depistarea și investigarea infracțiunilor.

(18) Participarea la căutarea și schimbul automatizat de evidențe ale poliției ar trebui să rămână voluntară. În cazul în care statele membre decid să participe, acestea ar trebui să aibă posibilitatea de a efectua interogări în bazele de date ale altor state membre, în spirit de reciprocitate, numai dacă pun la dispoziție propriile baze de date pentru interogări efectuate de celelalte state membre. Statele membre participante ar trebui să creeze registre ale bazelor de date naționale privind evidențele poliției. Statele membre ar trebui să fie cele care decid ce baze de date naționale instituite în scopul prevenirii, depistării și investigării infracțiunilor se utilizează pentru a crea registrele naționale de evidențe ale poliției. Respectivele registre includ date din bazele de date naționale pe care poliția le verifică în mod obișnuit atunci când primește cereri de informații din partea altor autorități de aplicare a legii. Prezentul regulament instituie sistemul european de inventariere a evidențelor poliției (EPRIS) în conformitate cu principiul protejării vieții private din faza de proiectare. Garanțiile privind protecția datelor includ pseudonimizarea, deoarece registrele și interogările nu conțin date cu caracter personal clare, ci serii alfanumerice. Este important ca EPRIS să împiedice statele membre sau Europol să inverseze pseudonimizarea și să dezvăluie datele de identificare care au generat corespondența. Având în vedere caracterul sensibil al datelor în cauză, schimburile de registre naționale de evidențe ale poliției în temeiul prezentului regulament ar trebui să vizeze numai datele persoanelor condamnate sau suspectate de a fi comis o infracțiune. În plus, ar trebui să fie posibilă efectuarea de căutări automatizate în registrele naționale de evidențe a poliției numai în scopul prevenirii, depistării și investigării unei infracțiuni pentru care se prevede pedeapsa cu închisoarea de cel puțin un an în temeiul dreptului statului membru solicitant.

(19) Schimbul de evidențe ale poliției în temeiul prezentului regulament nu aduce atingere schimbului de cazier judiciare prin intermediul cadrului în vigoare al Sistemului european de informații cu privire la cazierele judiciare (ECRIS) stabilit prin Decizia-cadru 2009/315/JAI a Consiliului ([11]).

(20) În ultimii ani, Europol a primit un volum mare de date biometrice ale suspecților și ale persoanelor condamnate pentru terorism și infracțiuni din partea autorităților țărilor terțe, în conformitate cu Regulamentul (UE) 2016/794, inclusiv informații de pe câmpul de luptă din zone de război. În multe cazuri nu a fost posibil ca aceste date să fie exploatate pe deplin, deoarece acestea nu se află întotdeauna la dispoziția autorităților competente din statele membre. Includerea datelor furnizate de țări terțe și stocate la nivelul Europol în cadrul Prüm II și, prin urmare, punerea acestor date la dispoziția autorităților competente ale statelor membre, în conformitate cu rolul Europol ca centru în materie de informații penale în Uniune, sunt necesare pentru o mai bună prevenire, depistare și investigare a infracțiunilor grave. Acestea contribuie, de asemenea, la crearea de sinergii între diferitele instrumente de asigurare a respectării legii și asigură că datele sunt utilizate în cel mai eficient mod cu putință.

(21) În temeiul cadrului Prüm II, Europol ar trebui să poată efectua căutări în bazele de date ale statelor membre cu date primite de la autoritățile țărilor terțe, cu respectarea deplină a normelor și condițiilor prevăzute în Regulamentul (UE) 2016/794, pentru a stabili legături transfrontaliere între cauzele penale cu privire la care Europol este competent. Posibilitatea de a utiliza datele Prüm, alături de alte baze de date aflate la dispoziția Europol, ar trebui să permită efectuarea unei analize mai complete și mai documentate, permițând astfel Europol să ofere un sprijin mai bun autorităților competente din statele membre pentru prevenirea, depistarea și investigarea infracțiunilor.

([11]) Decizia-cadru 2009/315/JAI a Consiliului din 26 februarie 2009 privind organizarea și conținutul schimbului de informații extrase din cazierele judiciare între statele membre (JO L 93, 7.4.2009, p. 23).

(22) Europol ar trebui să se asigure că solicitările sale de căutare nu depășesc capacitățile de căutare de date dactiloscopice și imagini faciale stabilite de statele membre. În cazul unei concordanțe între datele utilizate pentru căutare și datele stocate în bazele de date ale statelor membre, statele membre ar trebui să fie cele care decid dacă furnizează Europol informațiile necesare pentru îndeplinirea atribuțiilor sale.

(23) Regulamentul (UE) 2016/794 se aplică în întregime participării Europol la cadrul Prüm II. Orice utilizare de către Europol a datelor primite de la țări terțe este reglementată de articolul 19 din Regulamentul (UE) 2016/794. Orice utilizare de către Europol a datelor obținute în urma căutărilor automatizate în temeiul cadrului Prüm II ar trebui să facă obiectul consimțământului statului membru care a furnizat datele și este reglementată de articolul 25 din Regulamentul (UE) 2016/794 în cazul în care datele sunt transferate către țări terțe.

(24) Deciziile 2008/615/JAI și 2008/616/JAI prevăd o rețea de conexiuni bilaterale între bazele de date naționale ale statelor membre. Ca urmare a respectivei arhitecturi tehnice, fiecare stat membru a trebuit să stabilească o conexiune cu fiecare stat membru care participă la schimburi, ceea ce a însemnat cel puțin 26 de conexiuni pentru fiecare stat membru și pentru fiecare categorie de date. Routerul și EPRIS vor simplifica arhitectura tehnică a cadrului Prüm și vor servi drept puncte de legătură între toate statele membre. Routerul ar necesita o conexiune unică pentru fiecare stat membru în ceea ce privește datele biometrice, iar EPRIS ar necesita o conexiune unică pentru fiecare stat membru participant în ceea ce privește evidențele poliției.

(25) Routerul ar trebui să fie conectat la portalul european de căutare instituit prin Regulamentele (UE) 2019/817 ([12]) și (UE) 2019/818 ([13]) ale Parlamentului European și ale Consiliului, pentru a permite autorităților competente ale statelor membre și Europol să lanseze interogări în bazele de date naționale în temeiul prezentului regulament în același timp cu interogările în registrul comun de date de identitate instituit prin respectivele regulamente în scopul asigurării respectării legii, în conformitate cu respectivele regulamente. Așadar, este necesar ca aceste regulamente să fie modificate în consecință. În plus, Regulamentul (UE) 2019/818 ar trebui modificat pentru a permite stocarea rapoartelor și a statisticilor routerului în registrul central de raportare și statistici.

(26) Ar trebui să fie posibil ca un număr de referință pentru date biometrice să poată consta într-un număr de referință provizoriu sau într-un număr de control al operațiunii.

(27) Sistemele automatizate de identificare a amprentelor digitale și sistemele de recunoaștere a imaginii faciale utilizează modele biometrice compuse din date care provin dintr-o extracție de caracteristici din eșantioane biometrice reale. Modelele biometrice ar trebui obținute din date biometrice, însă nu ar trebui să fie posibil să se obțină aceleași date biometrice din modelele biometrice.

(28) În cazul în care statul membru solicitant decide astfel și dacă acest lucru este aplicabil în funcție de tipul de date biometrice, routerul ar trebui să clasifice răspunsurile statului membru solicitat sau ale statelor membre solicitate sau ale Europol, comparând datele biometrice utilizate pentru interogare și datele biometrice furnizate în răspunsurile statului membru solicitat sau ale statelor membre solicitate sau ale Europol.

(29) În cazul unei concordanțe între datele utilizate pentru căutare și datele deținute în baza de date națională a statului membru solicitat sau a statelor membre solicitate, după confirmarea manuală a concordanței de către un membru calificat al personalului statului membru solicitant și după transmiterea unei descrieri a faptelor și indicarea infracțiunii care justifică cererea, utilizând tabelul comun al categoriilor de infracțiuni prevăzut într-un act de punere în aplicare care urmează să fie adoptat în temeiul Deciziei-cadru 2009/315/JAI, statul membru solicitat ar trebui să returneze un set limitat de date de bază, în măsura în care astfel de date de bază sunt disponibile. Setul

([12]) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE în domeniul frontierelor și al vizelor și de modificare a Regulamentelor (CE) nr. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 și (UE) 2018/1861 ale Parlamentului European și ale Consiliului și a Deciziilor 2004/512/CE și 2008/633/JAI ale Consiliului (JO L 135, 22.5.2019, p. 27).

([13]) Regulamentul (UE) 2019/818 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE în domeniul cooperării polițienești și judiciare, al azilului și al migrației și de modificare a Regulamentelor (UE) 2018/1726, (UE) 2018/1862 și (UE) 2019/816 (JO L 135, 22.5.2019, p. 85).

limitat de date de bază ar trebui să fie returnat prin intermediul routerului în termen de 48 de ore de la îndeplinirea condițiilor relevante, cu excepția cazului în care este necesară o autorizație judiciară în temeiul dreptului intern. Respectivul termen va asigura un schimb rapid de informații între autoritățile competente ale statelor membre. Statele membre ar trebui să păstreze controlul asupra divulgării setului limitat de date de bază. Intervenția umană ar trebui menținută în momentele-cheie ale procesului, inclusiv în ceea ce privește decizia de a lansa o interogare, decizia de a confirma o concordanță, decizia de a lansa o cerere de primire a datelor de bază în urma unei concordanțe confirmate și decizia de a divulga date cu caracter personal statului membru solicitant, pentru a se asigura că datele de bază nu vor fi schimbate automatizat.

(30) În cazul specific al ADN-ului, statul membru solicitat ar trebui de asemenea să fie în măsură să confirme o concordanță între două profiluri ADN, atunci când acest lucru este relevant pentru investigarea infracțiunilor. După confirmarea respectivei concordanțe de către statul membru solicitat și după transmiterea unei descrieri a faptelor și indicarea infracțiunii care justifică cererea, utilizând tabelul comun al categoriilor de infracțiuni prevăzut într-un act de punere în aplicare care urmează să fie adoptat în conformitate cu Decizia-cadru 2009/315/JAI, statul membru solicitant ar trebui să returneze prin router un set limitat de date de bază, în termen de 48 de ore de la îndeplinirea condițiilor relevante, cu excepția cazului în care este necesară o autorizație judiciară în temeiul dreptului intern.

(31) Datele furnizate și primite în mod legal în temeiul prezentului regulament sunt supuse unor limitări în timp în ceea ce privește stocarea și revizuirea, stabilite în temeiul Directivei (UE) 2016/680.

(32) La dezvoltarea routerului și a EPRIS ar trebui utilizat standardul privind formatul universal pentru mesaje (*universal message format* – UMF), în măsura posibilului. Orice schimb automatizat de date în temeiul prezentului regulament ar trebui să utilizeze standardul UMF, în măsura posibilului. Autoritățile competente ale statelor membre și Europol sunt încurajate să utilizeze standardul UMF în legătură cu orice alt schimb de date între acestea în contextul cadrului Prüm II. Standardul UMF ar trebui să reprezinte un standard pentru schimburile de informații transfrontaliere structurate între sistemele de informații, autoritățile sau organizațiile din domeniul justiției și afacerilor interne.

(33) Doar informațiile neclasificate ar trebui să facă obiectul schimburilor prin intermediul cadrului Prüm II.

(34) Fiecare stat membru ar trebui să notifice celorlalte state membre, Comisiei, Agenției Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA), instituită prin Regulamentul (UE) 2018/1726 al Parlamentului European și al Consiliului ([14]), și Europol conținutul bazelor sale de date naționale puse la dispoziție prin intermediul cadrului Prüm II și condițiile pentru căutările automatizate.

(35) Anumite aspecte ale cadrului Prüm II nu pot fi reglementate în mod exhaustiv prin prezentul regulament, dată fiind natura lor tehnică, gradul lor de detaliu și necesitatea de a fi actualizate în mod regulat. Printre aceste aspecte se numără, de exemplu, modalitățile și specificațiile tehnice pentru procedurile de căutare automatizată, standardele pentru schimbul de date, inclusiv standardele minime de calitate, și elementele de date care urmează să facă obiectul schimbului. În vederea asigurării unor condiții uniforme de punere în aplicare a prezentului regulament în privința unor astfel de aspecte, ar trebui să fie conferite competențe de executare Comisiei. Respectivele competențe ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([15]).

(36) Calitatea datelor este extrem de importantă ca garanție și condiție prealabilă esențială pentru a garanta eficiența prezentului regulament. În contextul căutărilor automatizate de date biometrice și pentru a se garanta că datele transmise sunt de o calitate suficientă și a reduce riscul de false concordanțe, ar trebui stabilit un standard minim de calitate, care ar trebui revizuit periodic.

([14]) Regulamentul (UE) 2018/1726 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA) și de modificare a Regulamentului (CE) nr. 1987/2006 și a Deciziei 2007/533/JAI a Consiliului, precum și de abrogare a Regulamentului (UE) nr. 1077/2011 (JO L 295, 21.11.2018, p. 99).

([15]) Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

(37) Având în vedere amploarea și caracterul sensibil al datelor cu caracter personal transferate în sensul prezentului regulament, precum și existența unor dispoziții naționale diferite în ceea ce privește stocarea informațiilor privind persoanele fizice în bazele de date naționale, este important să se asigure faptul că bazele de date utilizate pentru căutarea automatizată în temeiul prezentului regulament sunt instituite în conformitate cu dreptul intern și cu Directiva (UE) 2016/680. Prin urmare, înainte de a-și conecta bazele de date naționale la router sau la EPRIS, statele membre ar trebui să efectueze o evaluare a impactului asupra protecției datelor, astfel cum se menționează în Directiva (UE) 2016/680 și, după caz, să consulte autoritatea de supraveghere prevăzută în directiva respectivă.

(38) Statele membre și Europol ar trebui să asigure acuratețea și relevanța datelor cu caracter personal prelucrate în temeiul prezentului regulament. În cazul în care un stat membru sau Europol constată că au fost furnizate date care sunt incorecte sau care nu mai sunt actualizate sau care nu ar fi trebuit furnizate, acesta ar trebui să notifice statul membru care a primit datele sau Europol, după caz, fără întârzieri nejustificate. Toate statele membre în cauză sau Europol, după caz, ar trebui să corecteze sau să șteargă datele în consecință, fără întârzieri nejustificate. În cazul în care statul membru care a primit datele sau Europol are motive să creadă că datele furnizate sunt incorecte sau ar trebui șterse, acesta ar trebui să informeze statul membru care a furnizat datele fără întârzieri nejustificate.

(39) Monitorizarea strictă a punerii în aplicare a prezentului regulament este extrem de importantă. În special, respectarea normelor privind prelucrarea datelor cu caracter personal ar trebui să facă obiectul unor garanții eficace și ar trebui asigurate monitorizări și audituri periodice realizate de către operatorii de date, autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor, după caz. Ar trebui să existe și dispoziții care să permită verificarea periodică a admisibilității interogărilor și a legalității prelucrării datelor.

(40) Autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor ar trebui să asigure supravegherea coordonată a aplicării prezentului regulament în cadrul responsabilităților lor, în special dacă identifică discrepanțe importante între practicile statelor membre sau transferuri potențial ilegale.

(41) În punerea în aplicare a prezentului regulament este esențial ca statele membre și Europol să ia act de jurisprudența Curții de Justiție a Uniunii Europene în ceea ce privește schimbul de date biometrice.

(42) La trei ani de la începerea funcționării routerului și a EPRIS și, ulterior, o dată la patru ani, Comisia ar trebui să elaboreze un raport de evaluare care să includă o evaluare a aplicării prezentului regulament de către statele membre și Europol, în special în ceea ce privește respectarea de către acestea a garanțiilor aplicabile în materie de protecție a datelor. Rapoartele de evaluare ar trebui să includă și o examinare a rezultatelor obținute în raport cu obiectivele prezentului regulament și a impactului acestuia asupra drepturilor fundamentale. Rapoartele de evaluare ar trebui să evalueze în același timp impactul, performanța, eficacitatea, eficiența, securitatea și practicile de lucru ale cadrului Prüm II.

(43) Întrucât prezentul regulament prevede instituirea unui nou cadru Prüm, dispozițiile Deciziilor 2008/615/JAI și 2008/616/JAI care nu mai sunt relevante ar trebui eliminate. Deciziile respective ar trebui să fie modificate în consecință.

(44) Întrucât routerul urmează să fie dezvoltat și gestionat de eu-LISA, Regulamentul (UE) 2018/1726 ar trebui să fie modificat prin adăugarea respectivei atribuții la sarcinile eu-LISA.

(45) Întrucât obiectivele prezentului regulament, și anume intensificarea cooperării polițienești transfrontaliere și mandatarea autorităților competente ale statelor membre să caute persoane dispărute și să identifice rămășițe umane neidentificate, nu pot fi realizate în mod satisfăcător de către statele membre, dar, având în vedere amploarea și efectele acțiunii, acestea pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană (TUE). În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivelor respective.

(46) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la TUE și la TFUE, Danemarca nu participă la adoptarea prezentului regulament, acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică.

(47) În conformitate cu articolul 3 din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la TUE și la TFUE, Irlanda a notificat intenția sa de a participa la adoptarea și la aplicarea prezentului regulament.

(48) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 și a emis un aviz la 2 martie 2022 ([16]),

ADOPTĂ PREZENTUL REGULAMENT:

*CAPITOLUL 1*

***Dispoziții generale***

*Articolul 1*

**Obiectul**

Prezentul regulament stabilește un cadru pentru căutarea și schimbul de informații între autoritățile competente din statele membre (denumit în continuare „cadrul Prüm II") prin stabilirea:

(a) condițiilor și procedurilor pentru căutarea automatizată de profiluri ADN, de date dactiloscopice, de anumite date privind înmatricularea vehiculelor, de imagini faciale și de evidențe ale poliției; și

(b) normelor privind schimbul de date de bază în urma unei concordanțe confirmate de date biometrice.

*Articolul 2*

**Scopul**

Scopul cadrului Prüm II este de a intensifica cooperarea transfrontalieră în domeniile reglementate de partea III titlul V capitolele 4 și 5 din Tratatul privind funcționarea Uniunii Europene, în special prin facilitarea schimbului de informații între autoritățile competente ale statelor membre, cu respectarea deplină a drepturilor fundamentale ale persoanelor fizice, inclusiv dreptul la viață privată și dreptul la protecția datelor cu caracter personal, în conformitate cu Carta drepturilor fundamentale a Uniunii Europene.

De asemenea, cadrul Prüm II are scopul de a le permite autorităților competente din statele membre să efectueze căutări ale persoanelor dispărute în contextul anchetelor penale sau din motive umanitare și să identifice rămășițe umane, în conformitate cu articolul 29, cu condiția ca autoritățile respective să fie împuternicite să efectueze astfel de căutări și să efectueze o astfel de identificare în temeiul dreptului intern.

*Articolul 3*

**Domeniul de aplicare**

Prezentul regulament se aplică bazelor de date instituite în conformitate cu dreptul intern și utilizate pentru transferul automatizat al profilurilor ADN, al datelor dactiloscopice, al anumitor date privind înmatricularea vehiculelor, al imaginilor faciale și al evidențelor poliției, în conformitate cu Directiva (UE) 2016/680 sau cu Regulamentul (UE) 2018/1725, (UE) 2016/794 sau (UE) 2016/679, după caz.

([16]) JO C 225, 9.6.2022, p. 6.

*Articolul 4*

**Definiții**

În sensul prezentului regulament, se aplică următoarele definiții:

1. „loci” (singular: „locus”) înseamnă segmente de ADN care conțin caracteristicile de identificare a unei mostre de ADN uman analizate;

2. „profil ADN” înseamnă un cod alfabetic sau numeric care reprezintă un set de loci sau structura moleculară specifică din diverși loci;

3. „date de referință ADN” înseamnă un profil ADN și numărul de referință menționat la articolul 7;

4. „profil ADN identificat” înseamnă profilul ADN al unei persoane identificate;

5. „profil ADN neidentificat” înseamnă profilul ADN colectat în cursul investigării unor infracțiuni și care aparține unei persoane încă neidentificate, inclusiv profilul ADN obținut din urme;

6. „date dactiloscopice” înseamnă imagini de amprente digitale, imagini de amprente digitale latente, imagini de amprente palmare, imagini de amprente palmare latente și șabloane ale unor astfel de imagini (caracteristici codificate ale acestora) care sunt stocate și prelucrate într-o bază de date automatizată;

7. „date dactiloscopice de referință” înseamnă date dactiloscopice și numărul de referință menționat la articolul 12;

8. „date dactiloscopice neidentificate” înseamnă datele dactiloscopice colectate în cursul investigării unei infracțiuni și care aparțin unei persoane neidentificate încă, inclusiv datele dactiloscopice obținute din urme;

9. „date dactiloscopice identificate” înseamnă datele dactiloscopice ale unei persoane identificate;

10. „caz individual” înseamnă un dosar unic legat de prevenirea, depistarea sau investigarea unei infracțiuni, de căutarea unei persoane dispărute sau de identificarea unor rămășițe umane neidentificate;

11. „imagine facială” înseamnă o imagine digitală a feței;

12. „date de referință privind imaginea facială” înseamnă o imagine facială și numărul de referință menționat la articolul 21;

13. „imagine facială neidentificată” înseamnă o imagine facială colectată în cursul investigării unei infracțiuni și care aparține unei persoane neidentificate încă, inclusiv o imagine facială obținută din urme;

14. „imagine facială identificată” înseamnă imaginea facială a unei persoane identificate;

15. „date biometrice” înseamnă profiluri ADN, date dactiloscopice sau imagini faciale;

16. „date alfanumerice” înseamnă date constând în litere, cifre, caractere speciale, spații și semne de punctuație;

17. „concordanță” înseamnă existența unei corespondențe care reiese din compararea automatizată a unor date cu caracter personal deținute într-o bază de date;

18. „candidat” înseamnă datele pentru care a survenit o concordanță;

19. „stat membru solicitant” înseamnă un stat membru care efectuează o căutare prin intermediul cadrului Prüm II;

20. „stat membru solicitat” înseamnă un stat membru în ale cărui baze de date un stat membru solicitant efectuează o căutare prin intermediul cadrului Prüm II;

21. „evidențe ale poliției” înseamnă date biografice ale suspecților și ale persoanelor condamnate, disponibile în bazele de date naționale instituite în scopul prevenirii, depistării și investigării infracțiunilor;

22. „pseudonimizare” înseamnă pseudonimizarea în înțelesul definiției de la articolul 3 punctul 5 din Directiva (UE) 2016/680;

23. „suspect” înseamnă o persoană astfel cum este menționată la articolul 6 litera (a) din Directiva (UE) 2016/680;

24. „date cu caracter personal” înseamnă datele cu caracter personal în înțelesul definiției de la articolul 3 punctul 1 din Directiva (UE) 2016/680;

25. „date Europol” înseamnă orice date operaționale cu caracter personal prelucrate de Europol în conformitate cu Regulamentul (UE) 2016/794;

26. „autoritate competentă” înseamnă orice autoritate publică competentă pentru prevenirea, depistarea sau investigarea infracțiunilor sau orice alt organism sau entitate însărcinată prin legislația statului membru cu exercitarea autorității publice și a prerogativelor publice în scopul prevenirii, depistării sau investigării infracțiunilor;

27. „autoritate de supraveghere” înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 41 din Directiva (UE) 2016/680;

28. „SIENA” înseamnă aplicația de rețea securizată pentru schimbul de informații, gestionată și dezvoltată de Europol în conformitate cu Regulamentul (UE) 2016/794;

29. „incident” înseamnă un incident în înțelesul definiției de la articolul 6 punctul 5 din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului ([17]).

30. „incident semnificativ” înseamnă orice incident, cu excepția cazului în care respectivul incident are un impact redus și este probabil să fie deja bine înțeles în ceea ce privește metoda sau tehnologia;

31. „amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică care are oportunitatea și vocația de a provoca un incident semnificativ, și care are un asemenea scop;

32. „vulnerabilitate semnificativă” înseamnă o vulnerabilitate care poate duce la un incident semnificativ dacă este exploatată.

*CAPITOLUL 2*

***Schimbul de date***

Secțiunea 1

**Profiluri ADN**

*Articolul 5*

**Date ADN de referință**

(1) Statele membre asigură disponibilitatea datelor de referință ADN din bazele lor de date ADN naționale în scopul efectuării de căutări automatizate de către alte state membre și de către Europol în temeiul prezentului regulament.

Datele de referință ADN nu conțin niciun fel de date suplimentare care să permită identificarea directă a unei persoane.

Profilurile ADN neidentificate trebuie să poată fi recunoscute ca atare.

(2) Datele ADN de referință se prelucrează în conformitate cu prezentul regulament și cu respectarea dreptului intern aplicabil procedurii de prelucrare a datelor respective.

([17]) Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80).

(3) Comisia adoptă un act de punere în aplicare pentru a preciza caracteristicile de identificare ale unui profil ADN care face obiectul schimbului de date. Respectivul act de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).

*Articolul 6*

**Căutarea automatizată a profilurilor ADN**

(1) În scopul investigării infracțiunilor, statele membre efectuează, la momentul primei conectări la router prin intermediul punctelor lor de contact naționale, o căutare automatizată, comparând toate profilurile ADN stocate în bazele lor de date ADN cu toate profilurile ADN stocate în bazele de date ADN ale tuturor celorlalte state membre și cu datele Europol. Fiecare stat membru convine la nivel bilateral cu fiecare alt stat membru și cu Europol cu privire la modalitățile de efectuare a respectivelor căutări automatizate, în conformitate cu normele și procedurile prevăzute în prezentul regulament.

(2) În scopul investigării infracțiunilor, statele membre, prin intermediul punctelor lor de contact naționale, efectuează căutări automatizate, comparând toate profilurile ADN nou adăugate în baza lor de date ADN cu toate profilurile ADN stocate în bazele de date ADN ale tuturor celorlalte state membre și cu datele Europol.

(3) În cazul în care căutările, astfel sunt menționate la alineatul (2), nu pot avea loc, statul membru în cauză poate conveni la nivel bilateral cu fiecare alt stat membru și cu Europol să le efectueze într-o etapă ulterioară, comparând profilurile ADN cu toate profilurile ADN stocate în bazele de date ADN ale tuturor celorlalte state membre și cu datele Europol. Statul membru în cauză convine la nivel bilateral cu fiecare alt stat membru și cu Europol cu privire la modalitățile de efectuare a respectivelor căutări automatizate, în conformitate cu normele și procedurile prevăzute în prezentul regulament.

(4) Căutările, astfel cum sunt menționate la alineatele (1), (2) și (3) se efectuează numai în cadrul unor cazuri individuale și în conformitate cu dreptul intern al statului membru solicitant.

(5) În cazul în care o căutare automatizată indică o concordanță între un profil ADN furnizat și un profil ADN stocat în baza de date sau în bazele de date ale statului membru solicitat în care se efectuează căutarea, punctul de contact național al statului membru solicitant primește o notificare automatizată a datelor de referință ADN în raport cu care a fost identificată o concordanță.

(6) Punctul de contact național al statului membru solicitant poate decide să confirme o concordanță între două profiluri ADN. Dacă decide să confirme o concordanță între două profiluri ADN, acesta informează statul membru solicitat și se asigură că se efectuează o revizuire manuală de către cel puțin un membru calificat al personalului pentru a confirma respectiva concordanță cu datele de referință ADN primite de la statul membru solicitat.

(7) Dacă este relevant în scopul investigării infracțiunilor, punctul de contact național al statului membru solicitat poate decide să confirme o concordanță între două profiluri ADN. Dacă decide să confirme o concordanță între două profiluri ADN, acesta informează statul membru solicitant și se asigură că se efectuează o revizuire manuală de către cel puțin un membru calificat al personalului pentru a confirma respectiva concordanță cu datele de referință ADN primite de la statul membru solicitant.

*Articolul 7*

**Numerele de referință pentru profilurile ADN**

Numerele de referință pentru profilurile ADN reprezintă combinația dintre:

(a) un număr de referință care permite statelor membre, în cazul unei concordanțe, să extragă date suplimentare și alte informații din bazele lor de date naționale ADN pentru a le furniza unuia, mai multor sau tuturor celorlalte state membre, în conformitate cu articolul 47, sau către Europol, în conformitate cu articolul 49 alineatul (6);

(b) un număr de referință care permite Europol ca, în cazul unei concordanțe, să extragă date suplimentare și alte informații în sensul articolului 48 alineatul (1) din prezentul regulament pentru a le furniza unuia, mai multor sau tuturor statelor membre, în conformitate cu Regulamentul (UE) 2016/794;

(c) un cod care indică statul membru care deține profilul ADN;

(d) un cod care indică dacă profilul ADN este un profil ADN identificat sau un profil ADN neidentificat.

*Articolul 8*

**Principii privind schimbul de profiluri ADN**

(1) Statele membre iau măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea datelor de referință ADN trimise către alte state membre sau Europol, inclusiv criptarea acestora. Europol ia măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea datelor de referință ADN trimise către state membre, inclusiv criptarea acestora.

(2) Fiecare stat membru și Europol se asigură că profilurile ADN pe care le transmite sunt de o calitate suficientă pentru a permite compararea automatizată. Comisia stabilește, prin intermediul actelor de punere în aplicare, un standard minim de calitate care să permită compararea profilurilor ADN.

(3) Comisia adoptă acte de punere în aplicare prin care precizează standardele europene sau internaționale relevante care trebuie utilizate de către statele membre și Europol pentru schimbul de date de referință ADN.

(4) Actele de punere în aplicare menționate la alineatele (2) și (3) de la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).

*Articolul 9*

**Norme privind solicitările și răspunsurile referitoare la profilurile ADN**

(1) O solicitare de căutare automatizată a profilurilor ADN include numai informațiile următoare:

(a) codul statului membru solicitant;

(b) data și ora solicitării și numărul solicitării;

(c) datele de referință ADN;

(d) dacă profilurile ADN transmise sunt profiluri ADN neidentificate sau profiluri ADN identificate.

(2) Un răspuns la o solicitare astfel cum este menționată la alineatul (1) conține numai informațiile următoare:

(a) o precizare din care să reiasă dacă a existat una sau au existat mai multe concordanțe sau dacă nu a existat nicio concordanță;

(b) data și ora solicitării și numărul solicitării;

(c) data și ora răspunsului și numărul răspunsului;

(d) codul statului membru solicitant și cel al statului membru solicitat;

(e) numerele de referință ale profilurilor ADN din statul membru solicitant și din statul membru solicitat;

(f) dacă profilurile ADN transmise sunt profiluri ADN neidentificate sau profiluri ADN identificate;

(g) profilurile ADN între care s-a stabilit o concordanță.

(3) O concordanță se notifică automat numai dacă în urma căutării automatizate a rezultat o concordanță cu un număr minim de loci. Comisia adoptă acte de punere în aplicare prin care precizează numărul minim de loci în acest scop, în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).

(4) În cazul în care o căutare de profiluri ADN neidentificate conduce la o concordanță, fiecare stat membru solicitat care deține date cu care s-a stabilit concordanța poate introduce în baza sa de date națională un marcaj care să indice că a existat o concordanță pentru profilul ADN respectiv în urma căutării efectuate de un alt stat membru. Marcajul include numărul de referință al profilului ADN utilizat de statul membru solicitant.

(5) Statele membre se asigură că solicitările menționate la alineatul (1) de la prezentul articol sunt corelate cu notificările transmise în temeiul articolului 74. Notificările respective se reproduc în manualul practic menționat la articolul 79.

Secțiunea 2

**Date dactiloscopice**

*Articolul 10*

**Date dactiloscopice de referință**

(1) Statele membre asigură disponibilitatea datelor dactiloscopice de referință din bazele lor de date naționale instituite în scopul prevenirii, depistării și investigării infracțiunilor.

(2) Datele dactiloscopice de referință nu conțin niciun fel de date suplimentare care să permită identificarea directă a unei persoane.

(3) Datele dactiloscopice neidentificate trebuie să poată fi recunoscute ca atare.

*Articolul 11*

**Căutarea automatizată a datelor dactiloscopice**

(1) În scopul prevenirii, depistării și investigării infracțiunilor, statele membre permit punctelor de contact naționale ale altor state membre și Europol accesul la datele dactiloscopice de referință din bazele lor de date naționale pe care le-au instituit în acest scop, pentru a efectua căutări automatizate prin compararea datelor dactiloscopice de referință.

Căutările menționate la primul paragraf se efectuează numai în contextul unor cazuri individuale și în conformitate cu dreptul intern al statului membru solicitant.

(2) Punctul de contact național al statului membru solicitant poate decide să confirme o concordanță între două seturi de date dactiloscopice. Dacă decide să confirme o concordanță între două seturi de date dactiloscopice, acesta informează statul membru solicitat și se asigură că se efectuează o revizuire manuală de către cel puțin un membru calificat al personalului pentru a confirma respectiva concordanță cu datele dactiloscopice de referință primite de la statul membru solicitat.

*Articolul 12*

**Numerele de referință pentru datele dactiloscopice**

Numerele de referință pentru datele dactiloscopice reprezintă combinația dintre următoarele:

(a) un număr de referință care permite statelor membre, în cazul unei concordanțe, să extragă date suplimentare și alte informații din bazele lor de date menționate la articolul 10 pentru a le furniza unuia, mai multor sau tuturor celorlalte state membre, în conformitate cu articolul 47, sau către Europol, în conformitate cu articolul 49 alineatul (6);

(b) un număr de referință care permite Europol, în cazul unei concordanțe, să extragă date suplimentare și alte informații în sensul articolului 48 alineatul (1) din prezentul regulament pentru a le furniza unuia, mai multor sau tuturor statelor membre, în conformitate cu Regulamentul (UE) 2016/794;

(c) un cod care indică statul membru care deține datele dactiloscopice.

*Articolul 13*

**Principii privind schimbul de date dactiloscopice**

(1) Statele membre iau măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea datelor dactiloscopice trimise altor state membre sau Europol, inclusiv criptarea acestora. Europol ia măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea datelor dactiloscopice trimise statelor membre, inclusiv criptarea acestora.

(2) Fiecare stat membru și Europol se asigură că datele dactiloscopice pe care le transmite sunt de o calitate suficientă pentru a permite compararea automatizată. Comisia stabilește, prin intermediul actelor de punere în aplicare, un standard minim de calitate care să permită compararea datelor dactiloscopice.

(3) Datele dactiloscopice se digitalizează și se transmit către celelalte state membre sau către Europol în conformitate cu standardele europene sau internaționale. Comisia adoptă acte de punere în aplicare prin care precizează standardele europene sau internaționale relevante care trebuie utilizate de statele membre și Europol pentru schimbul de date dactiloscopice.

(4) Acte de punere în aplicare menționate în alineatele (2) și (3) de la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).

*Articolul 14*

**Capacități de căutare pentru datele dactiloscopice**

(1) Fiecare stat membru se asigură că solicitările sale de căutare nu depășesc capacitățile de căutare precizate de statul membru solicitat sau de Europol, pentru a asigura disponibilitatea sistemului și pentru a evita supraîncărcarea sistemului. În același scop, Europol se asigură că solicitările sale de căutare nu depășesc capacitățile de căutare precizate de statul membru solicitat.

Statele membre informează celelalte state membre, Comisia, eu-LISA și Europol cu privire la capacitățile lor maxime de căutare pe zi pentru datele dactiloscopice ale persoanelor identificate și neidentificate. Europol informează statele membre, Comisia și eu-LISA cu privire la capacitățile lor maxime de căutare pe zi pentru datele dactiloscopice ale persoanelor identificate și neidentificate. Statele membre sau Europol pot majora în mod temporar sau permanent respectivele capacități de căutare în orice moment, inclusiv în cazul unei urgențe. Dacă un stat membru își majorează respectivele capacități maxime de căutare, notifică celorlalte state membre, Comisiei, eu-LISA și Europol noile capacități maxime de căutare. Dacă Europol își majorează respectivele capacități maxime de căutare, notifică statelor membre, Comisiei și eu-LISA noile capacități maxime de căutare.

(2) Comisia adoptă acte de punere în aplicare prin care precizează numărul maxim de candidați acceptați pentru comparație pentru fiecare transmitere și distribuția capacităților de căutare nefolosite între statele membre, în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).

*Articolul 15*

**Norme privind solicitările și răspunsurile referitoare la datele dactiloscopice**

(1) O solicitare de căutare automatizată de date dactiloscopice include numai informațiile următoare:

(a) codul statului membru solicitant;

(b) data și ora solicitării și numărul solicitării;

(c) datele dactiloscopice de referință.

(2) Un răspuns la o solicitare astfel cum este menționată la alineatul (1) conține numai informațiile următoare:

(a) o precizare din care să reiasă dacă a existat una sau au existat mai multe concordanțe sau dacă nu a existat nicio concordanță;

(b) data și ora solicitării și numărul solicitării;

(c) data și ora răspunsului și numărul răspunsului;

(d) codul statului membru solicitant și cel al statului membru solicitat;

(e) numerele de referință ale datelor dactiloscopice din statul membru solicitant și din statul membru solicitat;

(f) datele dactiloscopice între care s-a stabilit o concordanță.

(3) Statele membre se asigură că solicitările menționate la alineatul (1) de la prezentul articol sunt corelate cu notificările transmise în temeiul articolului 74. Notificările respective se reproduc în manualul practic menționat la articolul 79.

Secțiunea 3

**Date privind înmatricularea vehiculelor**

*Articolul 16*

**Căutarea automatizată a datelor privind înmatricularea vehiculelor**

(1) În scopul prevenirii, depistării și investigării infracțiunilor, statele membre permit punctelor de contact naționale ale altor state membre și Europol accesul la următoarele date naționale privind înmatricularea vehiculelor, pentru a efectua căutări automatizate în cazuri individuale:

(a) datele referitoare la proprietar sau la deținătorul vehiculului;

(b) datele referitoare la vehicul.

(2) Căutările menționate la alineatul (1) se efectuează doar prin utilizarea următoarelor date:

(a) un număr complet de șasiu;

(b) un număr complet de înmatriculare; sau

(c) datele referitoare la proprietarul sau deținătorul vehiculului, în cazul în care acest lucru este autorizat de dreptul intern al statului membru solicitat.

(3) Căutările menționate la alineatul (1) efectuate cu datele referitoare la proprietarul sau deținătorul vehiculului se efectuează numai în cazul persoanelor suspectate sau condamnate. În scopul acestor căutări, se utilizează toate datele de identificare următoare:

(a) în cazul în care proprietarul sau deținătorul vehiculului este o persoană fizică:

  (i) prenumele persoanei fizice;

  (ii) numele de familie al persoanei fizice; și

  (iii) data nașterii persoanei fizice;

(b) în cazul în care proprietarul sau deținătorul vehiculului este o persoană juridică, denumirea persoanei juridice respective.

(4) Căutările menționate la alineatul (1) pot fi efectuate numai în conformitate cu dreptul intern al statului membru solicitant.

*Articolul 17*

**Principii de căutare automatizată a datelor privind înmatricularea vehiculelor**

(1) Pentru căutarea automatizată a datelor privind înmatricularea vehiculelor, statele membre utilizează Sistemul de informații european privind vehiculele și permisele de conducere (Eucaris).

(2) Informațiile schimbate prin Eucaris se transmit într-o formă criptată.

(3) Comisia adoptă acte de punere în aplicare prin care precizează elementele datelor privind înmatricularea vehiculelor care pot face obiectul schimburilor și procedura tehnică prin care Eucaris poate accesa bazele de date ale statelor membre. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).

*Articolul 18*

**Păstrarea înregistrărilor**

(1) Fiecare stat membru păstrează înregistrări ale interogărilor efectuate de personalul autorităților sale competente, autorizat în mod corespunzător să facă schimb de date privind înmatricularea vehiculelor, precum și înregistrări ale interogărilor solicitate de alte state membre. Europol păstrează înregistrări ale interogărilor efectuate de personalul său autorizat în mod corespunzător.

Fiecare stat membru și Europol păstrează înregistrări ale tuturor operațiunilor de prelucrare de date privind înmatricularea vehiculelor. În aceste înregistrări se includ următoarele informații:

(a) dacă un stat membru sau Europol a lansat solicitarea de interogare; dacă un stat membru a lansat solicitarea de interogare, se indică statul membru în cauză;

(b) data și ora solicitării;

(c) data și ora răspunsului;

(d) bazele de date naționale către care a fost trimisă o solicitare de interogare;

(e) bazele de date naționale care au oferit un răspuns pozitiv.

(2) Înregistrările menționate la alineatul (1) sunt utilizate numai pentru colectarea de statistici, pentru monitorizarea protecției datelor, inclusiv verificarea admisibilității unei interogări și a legalității prelucrării datelor, precum și pentru asigurarea securității și integrității datelor. Respectivele înregistrări se protejează prin măsuri corespunzătoare împotriva accesului neautorizat și se șterg după o perioadă de trei ani de la data la care au fost create. Dacă înregistrările sunt însă necesare pentru desfășurarea unor proceduri de monitorizare deja inițiate, acestea se șterg în momentul în care nu mai sunt necesare pentru procedurile de monitorizare.

(3) În scopul monitorizării protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, operatorii de date au acces la înregistrări pentru automonitorizarea menționată la articolul 55.

Secțiunea 4

**Imagini faciale**

*Articolul 19*

**Date de referință privind imaginile faciale**

(1) Statele membre asigură disponibilitatea datelor de referință privind imaginile faciale ale suspecților, ale persoanelor condamnate și, în cazul în care dreptul intern permite acest lucru, ale victimelor, din bazele lor de date naționale create pentru prevenirea, depistarea și investigarea infracțiunilor.

(2) Datele de referință privind imaginile faciale nu conțin niciun fel de date suplimentare care să permită identificarea directă a unei persoane.

(3) Imaginile faciale neidentificate sunt recunoscute ca atare.

*Articolul 20*

**Căutarea automatizată a imaginilor faciale**

(1) În scopul prevenirii, depistării și investigării infracțiunilor pentru care este prevăzută o pedeapsă maximă cu închisoarea de cel puțin un an în temeiul dreptului statului membru solicitant, statele membre permit punctelor de contact naționale ale altor state membre și Europol accesul la datele de referință privind imaginile faciale stocate în bazele lor de date naționale, pentru a efectua căutări automatizate.

Căutările menționate la primul paragraf se efectuează numai în contextul unor cazuri individuale și în conformitate cu dreptul intern al statului membru solicitant.

Crearea de profiluri astfel cum este menționată la articolul 11 alineatul (3) din Directiva (UE) 2016/680 este interzisă.

(2) Punctul de contact național al statului membru solicitant poate decide să confirme o concordanță între două imagini faciale. Dacă decide să confirme o concordanță între două imagini faciale, acesta informează statul membru solicitat și se asigură că se efectuează o revizuire manuală a listei de către cel puțin un membru calificat al personalului pentru a confirma această concordanță cu datele de referință privind imaginile faciale primite de la statul membru solicitat.

*Articolul 21*

**Numerele de referință pentru imaginile faciale**

Numerele de referință pentru imaginile faciale reprezintă combinația dintre următoarele:

(a) un număr de referință care permite statelor membre, în cazul unei concordanțe, să extragă date suplimentare și alte informații din bazele lor de date menționate la articolul 19 pentru a le furniza unuia, mai multor sau tuturor celorlalte state membre, în conformitate cu articolul 47, sau către Europol, în conformitate cu articolul 49 alineatul (6);

(b) un număr de referință care permite Europol, în cazul unei concordanțe, să extragă date suplimentare și alte informații în sensul articolului 48 alineatul (1) din prezentul regulament pentru a le furniza unuia, mai multor sau tuturor statelor membre, în conformitate cu Regulamentul (UE) 2016/794;

(c) un cod care indică statul membru care deține imaginile faciale.

*Articolul 22*

**Principii privind schimbul de imagini faciale**

(1) Statele membre iau măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea imaginilor faciale trimise altor state membre sau Europol, inclusiv criptarea acestora. Europol ia măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea imaginilor faciale trimise statelor membre, inclusiv criptarea acestora.

(2) Fiecare stat membru și Europol se asigură că imaginile faciale pe care le transmite sunt de o calitate suficientă pentru a permite compararea automatizată. Comisia stabilește, prin intermediul actelor de punere în aplicare, un standard minim de calitate care să permită compararea imaginilor faciale. Dacă raportul menționat la articolul 80 alineatul (7) indică un risc ridicat de concordanțe false, Comisia revizuiește actele de punere în aplicare respective.

(3) Comisia adoptă acte de punere în aplicare prin care precizează standardele relevante europene sau internaționale pentru schimbul de imagini faciale care trebuie să fie utilizate de statele membre și de Europol.

(4) Actele de punere în aplicare menționate în alineatele (2) și (3) de la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).

*Articolul 23*

**Capacitățile de căutare a imaginilor faciale**

(1) Fiecare stat membru se asigură că solicitările sale de căutare nu depășesc capacitățile de căutare specificate de statul membru solicitat sau de Europol pentru a asigura disponibilitatea sistemului și pentru a evita supraîncărcarea sistemului. În același scop, Europol se asigură că solicitările sale de căutare nu depășesc capacitățile de căutare specificate de statul membru solicitat.

Statele membre informează celelalte state membre, Comisia, eu-LISA și Europol cu privire la capacitățile lor maxime de căutare pe zi pentru schimburile de imagini faciale identificate sau neidentificate. Europol informează statele membre, Comisia și eu-LISA cu privire la capacitățile sale maxime de căutare pe zi pentru schimburile de imagini faciale identificate și neidentificate. Statele membre sau Europol pot majora în mod temporar sau permanent respectivele capacități de căutare în orice moment, inclusiv în cazul unei urgențe. Dacă un stat membru își majorează respectivele capacități maxime de căutare, notifică celorlalte state membre, Comisiei, eu-LISA și Europol noile capacități maxime de căutare. Dacă Europol își majorează respectivele capacități maxime de căutare, notifică statelor membre, Comisiei și eu-LISA noile capacități maxime de căutare.

(2) Comisia adoptă acte de punere în aplicare prin care precizează numărul maxim de candidați acceptați pentru comparație pentru fiecare transmitere și distribuția capacităților de căutare nefolosite între statele membre, în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).

*Articolul 24*

**Norme privind solicitările și răspunsurile referitoare la imaginile faciale**

(1) O solicitare de căutare automatizată de imagini faciale include numai informațiile următoare:

(a) codul statului membru solicitant;

(b) data și ora solicitării și numărul solicitării;

(c) datele de referință privind imaginile faciale.

(2) Un răspuns la o solicitare astfel cum este menționată la alineatul (1) conține numai informațiile următoare:

(a) o precizare din care să reiasă dacă a existat una sau au existat mai multe concordanțe sau dacă nu a existat nicio concordanță;

(b) data și ora solicitării și numărul solicitării;

(c) data și ora răspunsului și numărul răspunsului;

(d) codul statului membru solicitant și cel al statului membru solicitat;

(e) numerele de referință ale imaginilor faciale din statul membru solicitant și din statul membru solicitat;

(f) imaginile faciale între care s-a stabilit o concordanță.

(3) Statele membre se asigură că solicitările menționate la alineatul (1) de la prezentul articol sunt corelate cu notificările transmise în temeiul articolului 74. Notificările respective se reproduc în manualul practic menționat la articolul 79.

Secțiunea 5

**Evidențe ale poliției**

*Articolul 25*

**Evidențe ale poliției**

(1) Statele membre pot participa la schimbul automatizat de evidențe ale poliției. În scopul unor astfel de schimburi, statele membre participante asigură accesul la registrele naționale de evidențe ale poliției care conțin seturi de date biografice ale suspecților și ale persoanelor condamnate din bazele lor de date naționale create pentru prevenirea, depistarea și investigarea infracțiunilor. Respectivele seturi de date conțin numai următoarele date, în măsura în care sunt disponibile:

(a) prenumele;

(b) numele;

(c) pseudonimul sau pseudonimele și numele utilizat sau numele utilizate anterior;

(d) data nașterii;

(e) cetățenia sau cetățeniile;

(f) țara nașterii;

(g) genul.

(2) Datele menționate la alineatul (1) literele (a), (b), și (c) trebuie să fie pseudonimizate.

*Articolul 26*

**Căutarea automatizată în registrele naționale de evidențe ale poliției**

În scopul prevenirii, depistării și investigării infracțiunilor pentru care este prevăzută o pedeapsă maximă cu închisoarea de cel puțin un an în temeiul dreptului statului membru solicitant, statele membre participante la schimbul automatizat de evidențe ale poliției permit punctelor de contact naționale ale altor state membre participante și Europol accesul la datele din registrele naționale de evidențe ale poliției, pentru a efectua căutări automatizate.

Căutările menționate la primul paragraf se efectuează numai în contextul unor cazuri individuale și în conformitate cu dreptul intern al statului membru solicitant.

*Articolul 27*

**Numerele de referință pentru evidențele poliției**

Numerele de referință pentru evidențele poliției reprezintă combinația dintre următoarele:

(a) un număr de referință care permite statelor membre, în cazul unei concordanțe, să extragă date biografice și alte informații din registrele de evidențe ale poliției menționate la articolul 25 pentru a le furniza unuia, mai multor sau tuturor celorlalte state membre, în conformitate cu articolul 44;

(b) un cod care indică statul membru care deține evidențele poliției.

*Articolul 28*

**Norme privind solicitările și răspunsurile referitoare la evidențele poliției**

(1) O solicitare de căutare automatizată în registrele naționale de evidențe ale poliției include numai informațiile următoare:

(a) codul statului membru solicitant;

(b) data și ora solicitării și numărul solicitării;

(c) datele menționate la articolul 25, în măsura în care sunt disponibile.

(2) Un răspuns la o solicitare astfel cum este menționată la alineatul (1) conține numai informațiile următoare:

(a) o precizare a numărului de concordanțe;

(b) data și ora solicitării și numărul solicitării;

(c) data și ora răspunsului și numărul răspunsului;

(d) codul statului membru solicitant și cel al statului membru solicitat;

(e) numerele de referință ale evidențelor poliției din statele membre solicitate.

(3) Statele membre se asigură că solicitările menționate la alineatul (1) de la prezentul articol sunt corelate cu notificările transmise în temeiul articolului 74. Notificările respective se reproduc în manualul practic menționat la articolul 79.

Secțiunea 6

**Dispoziții comune**

*Articolul 29*

**Persoane dispărute și rămășițe umane neidentificate**

(1) Dacă o autoritate națională are competențe în acest sens în temeiul unor măsuri legislative naționale, astfel cum se menționează la alineatul (2), aceasta poate efectua căutări automatizate prin intermediul cadrului Prüm II exclusiv în scopul:

(a) căutării persoanelor dispărute în contextul anchetelor penale sau din motive umanitare;

(b) identificării de rămășițe umane.

(2) Statele membre care doresc să facă uz de posibilitatea prevăzută la alineatul (1) desemnează, prin intermediul unor măsuri legislative naționale, autoritățile naționale competente în scopurile prevăzute în astfel de măsuri și stabilesc proceduri, condiții și criterii, inclusiv motivele umanitare pentru care este permis să se efectueze căutări automatizate ale persoanelor dispărute astfel cum se menționează la alineatul (1) litera (a).

*Articolul 30*

**Puncte de contact naționale**

Fiecare stat membru desemnează unul sau mai multe puncte de contact naționale în sensul articolelor 6, 11, 16, 20 și 26.

*Articolul 31*

**Măsuri de punere în aplicare**

Comisia adoptă acte de punere în aplicare prin care precizează modalitățile tehnice pentru statele membre cu privire la procedurile prevăzute la articolele 6, 11, 16, 20 și 26. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).

*Articolul 32*

**Disponibilitatea schimbului automatizat de date la nivel național**

(1) Statele membre iau toate măsurile necesare pentru a asigura posibilitatea efectuării de căutări automatizate de profiluri ADN, de date dactiloscopice, de anumite date privind înmatricularea vehiculelor, de imagini faciale și de evidențe ale poliției timp de 24 de ore pe zi, 7 zile pe săptămână.

(2) Punctele de contact naționale se informează reciproc și informează Comisia, eu-LISA și Europol, fără întârziere, cu privire la orice indisponibilitate a schimbului automatizat de date, inclusiv, după caz, cu privire la orice defecțiuni tehnice care cauzează această indisponibilitate.

Punctele de contact naționale convin, în conformitate cu dreptul aplicabil al Uniunii și cu dreptul intern aplicabil, asupra unor modalități alternative temporare pentru schimbul de informații, care să fie utilizate în cazurile în care schimbul automatizat de date nu este disponibil.

(3) Atunci când schimbul automatizat de date nu este disponibil, punctele de contact naționale se asigură că acesta este restabilit, prin orice mijloace necesare fără întârziere.

*Articolul 33*

**Justificarea prelucrării datelor**

(1) Fiecare stat membru păstrează o evidență a justificărilor pentru interogările pe care le efectuează autoritățile sale competente.

Europol păstrează o evidență a justificărilor pentru interogările pe care le efectuează.

(2) Justificările menționate la alineatul (1) cuprind:

(a) scopul interogării, inclusiv o referire la cazul sau ancheta respectivă, și, după caz, infracțiunea specifică;

(b) o precizare dacă interogarea se referă la un suspect sau la o persoană condamnată pentru comiterea unei infracțiuni, la o victimă a unei infracțiuni, la o persoană dispărută sau la rămășițe umane neidentificate;

(c) o precizare dacă interogarea vizează identificarea unei persoane sau obținerea mai multor date cu privire la o persoană cunoscută.

(3) Justificările menționate la alineatul (1) de la prezentul articol trebuie să poată fi urmărite până la înregistrările menționate la articolele 18, 40 și 45. Respectivele justificări se pot utiliza numai pentru a evalua în ce măsură căutările sunt proporționale și necesare în scopul prevenirii, depistării sau investigării unei infracțiuni, pentru monitorizarea protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, precum și pentru asigurarea securității și integrității datelor. Respectivele justificări se protejează prin măsuri corespunzătoare împotriva accesului neautorizat și se șterg după o perioadă de trei ani de la data la care au fost create. Dacă înregistrările sunt însă necesare pentru desfășurarea unor proceduri de monitorizare aflate în curs, acestea se șterg odată ce nu mai sunt necesare pentru procedurile de monitorizare.

(4) Pentru evaluarea proporționalității și a necesității căutărilor în scopul prevenirii, depistării și investigării unei infracțiuni sau al monitorizării protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, operatorii de date au acces la respectivele justificări pentru automonitorizarea menționată la articolul 55.

*Articolul 34*

**Utilizarea formatului universal pentru mesaje**

(1) În măsura în care este posibil, la dezvoltarea routerului menționat la articolul 35 din prezentul regulament și a Sistemului european de inventariere a evidențelor poliției (EPRIS) se utilizează standardul privind formatul universal pentru mesaje (UMF) instituit prin articolul 38 din Regulamentul (UE) 2019/818.

(2) Orice schimb automatizat de date în conformitate cu prezentul regulament utilizează standardul UMF, în măsura în care este posibil.

*CAPITOLUL 3*

***Arhitectura***

Secțiunea 1

**Routerul**

*Articolul 35*

**Routerul**

(1) Se creează un router cu scopul de a facilita stabilirea de conexiuni între statele membre și între statele membre și Europol pentru interogarea, extragerea și evaluarea datelor biometrice și pentru extragerea datelor alfanumerice în conformitate cu prezentul regulament.

(2) Routerul este alcătuit din următoarele elemente:

(a) o infrastructură centrală, care include un instrument de căutare ce permite interogarea simultană a bazelor de date naționale menționate la articolele 5, 10 și 19, precum și a datelor Europol;

(b) un canal securizat de comunicații între infrastructura centrală, autoritățile competente autorizate să utilizeze routerul în temeiul articolului 36 și Europol;

(c) o infrastructură de comunicații securizată între infrastructura centrală și portalul european de căutare, instituit prin articolul 6 din Regulamentul (UE) 2019/817 și articolul 6 din Regulamentul (UE) 2019/818, în sensul articolului 39.

*Articolul 36*

**Utilizarea routerului**

Utilizarea routerului este rezervată autorităților competente ale statelor membre care sunt autorizate să acceseze și să facă schimbul de profiluri ADN, de date dactiloscopice și de imagini faciale în conformitate cu prezentul regulament, precum și Europol, în conformitate cu prezentul regulament și cu Regulamentul (UE) 2016/794.

*Articolul 37*

**Procedură**

(1) Autoritățile competente autorizate să utilizeze routerul în temeiul articolului 36 sau Europol solicită o interogare prin transmiterea de date biometrice către router. Routerul trimite solicitarea de interogare către bazele de date ale tuturor sau anumitor state membre și către datele Europol simultan cu datele transmise de utilizator în conformitate cu drepturile sale de acces.

(2) La primirea unei solicitări de interogare din partea routerului, fiecare stat membru solicitat lansează o interogare în bazele lor de date în mod automatizat și fără întârziere. La primirea unei solicitări de interogare din partea routerului, Europol lansează o interogare în datele Europol în mod automatizat și fără întârziere.

(3) Toate concordanțele rezultate în urma interogărilor astfel cum se menționează la alineatul (2) sunt trimise înapoi în mod automatizat routerului. Statul membru solicitant este informat în mod automat în cazul în care nu există nicio concordanță.

(4) Dacă statul membru solicitant decide astfel și dacă acest lucru este aplicabil, routerul clasifică răspunsurile comparând datele biometrice utilizate pentru interogare și datele biometrice furnizate în răspunsurile din partea statului membru solicitat sau a statelor membre solicitate sau ale Europol.

(5) Routerul returnează utilizatorului routerului lista datelor biometrice între care s-a stabilit o concordanță și clasificarea acestora.

(6) Comisia adoptă acte de punere în aplicare prin care precizează procedura tehnică pentru interogarea de către router a bazelor de date ale statelor membre și a datelor Europol, formatul în care routerul răspunde la astfel de interogări și normele tehnice pentru compararea și clasificarea corespondenței dintre datele biometrice. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).

*Articolul 38*

**Verificarea calității**

Statul membru solicitat verifică calitatea datelor transmise printr-o procedură automatizată.

Statul membru solicitat informează, fără întârziere, statul membru solicitant prin intermediul routerului atunci când datele sunt necorespunzătoare pentru a se efectua o comparare automatizată.

*Articolul 39*

**Interoperabilitatea dintre router și registrul comun de date de identitate în scopul accesului autorităților de aplicare a legii**

(1) Atunci când autoritățile desemnate, astfel cum sunt definite la articolul 4 punctul 20 din Regulamentul (UE) 2019/817 și la articolul 4 punctul 20 din Regulamentul (UE) 2019/818 sunt autorizate să utilizeze routerul în temeiul articolului 36 din prezentul regulament, acestea pot lansa o interogare în bazele de date ale statelor membre și în datele Europol simultan cu o interogare în registrul comun de date de identitate, instituit prin articolul 17 din Regulamentul (UE) 2019/817 și articolul 17 din Regulamentul (UE) 2019/818, cu condiția să fie îndeplinite condițiile relevante prevăzute de dreptul Uniunii și ca interogarea să fie lansată în conformitate cu drepturile lor de acces. În acest scop, routerul efectuează interogări în registrul comun de date de identitate prin intermediul portalului european de căutare.

(2) Interogările în registrul comun de date de identitate în scopul asigurării respectării legii se efectuează în conformitate cu articolul 22 din Regulamentul (UE) 2019/817 și cu articolul 22 din Regulamentul (UE) 2019/818. Orice rezultat al unor astfel de interogări se transmite prin intermediul portalului european de căutare.

Interogările simultane în bazele de date ale statelor membre și în datele Europol și în registrul comun de date de identitate sunt lansate numai atunci când există motive rezonabile să se considere că date privind un suspect, un autor sau o victimă a unei infracțiuni de terorism sau a unei alte infracțiuni grave, astfel cum sunt definite la articolul 4 punctele 21 și 22 din Regulamentul (UE) 2019/817 și, respectiv, la articolul 4 punctele 21 și 22 din Regulamentul (UE) 2019/818, sunt stocate în registrul comun de date de identitate.

*Articolul 40*

**Păstrarea înregistrărilor**

(1) eu-LISA păstrează înregistrări ale tuturor operațiunilor de prelucrare de date efectuate în router. Respectivele înregistrări includ următoarele informații:

(a) dacă un stat membru sau Europol a lansat solicitarea de interogare; dacă un stat membru a lansat solicitarea de interogare, se indică statul membru în cauză;

(b) data și ora solicitării;

(c) data și ora răspunsului;

(d) bazele de date naționale sau datele Europol către care a fost trimisă o solicitare de interogare;

(e) bazele de date naționale sau datele Europol care au oferit un răspuns;

(f) după caz, faptul că a existat o interogare simultană în registrul comun de date de identitate.

(2) Fiecare stat membru păstrează înregistrări ale interogărilor efectuate de personalul autorităților sale competente autorizat în mod corespunzător să utilizeze routerul, precum și înregistrări ale interogărilor solicitate de alte state membre.

Europol păstrează înregistrări ale interogărilor efectuate de personalul său autorizat în mod corespunzător.

(3) Înregistrările menționate la alineatele (1) și (2) sunt utilizate numai pentru colectarea de statistici și pentru monitorizarea protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, precum și pentru asigurarea securității și integrității datelor. Respectivele înregistrări se protejează prin măsuri corespunzătoare împotriva accesului neautorizat și se șterg după o perioadă de trei ani de la data la care au fost create. Dacă înregistrările sunt însă necesare pentru desfășurarea unor proceduri de monitorizare deja inițiate, acestea se șterg în momentul în care nu mai sunt necesare pentru procedurile de monitorizare.

(4) În scopul monitorizării protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, operatorii de date au acces la înregistrări pentru automonitorizarea menționată la articolul 55.

*Articolul 41*

**Proceduri de notificare în cazul imposibilității tehnice de a utiliza routerul**

(1) În cazul în care este imposibil din punct de vedere tehnic să se utilizeze routerul pentru a efectua interogări în una sau mai multe baze de date naționale sau în datele Europol din cauza unei defecțiuni a routerului, eu-LISA notifică utilizatorii routerului menționați la articolul 36, în mod automatizat. eu-LISA ia măsuri corespunzătoare pentru a soluționa imposibilitatea tehnică de a utiliza routerul.

(2) În cazul în care este imposibil din punct de vedere tehnic să se utilizeze routerul pentru a efectua interogări în una sau mai multe baze de date naționale din cauza unei defecțiuni a infrastructurii naționale dintr-un stat membru, statul membru respectiv notifică acest lucru celorlalte state membre, Comisiei, eu-LISA și Europol în mod automatizat. Statul membru vizat ia măsuri corespunzătoare fără întârziere pentru a soluționa imposibilitatea tehnică de a utiliza routerul.

(3) În cazul în care este imposibil din punct de vedere tehnic să se utilizeze routerul pentru a efectua interogări în datele Europol din cauza unei defecțiuni a infrastructurii Europol, Europol notifică acest lucru statelor membre, Comisiei și eu-LISA în mod automatizat. Europol ia măsuri corespunzătoare fără întârziere pentru a soluționa imposibilitatea tehnică de a utiliza routerul.

Secțiunea 2

**EPRIS**

*Articolul 42*

**EPRIS**

(1) Se stabilește Sistemul european de inventariere a evidențelor poliției (EPRIS). Pentru căutarea automatizată în registrele naționale ale evidențelor poliției menționate la articolul 26, statele membre și Europol utilizează EPRIS.

(2) EPRIS este alcătuit din:

(a) o infrastructură descentralizată în statele membre, care include un instrument de căutare care permite interogarea simultană a registrelor naționale ale evidențelor poliției, pe baza bazelor de date naționale;

(b) o infrastructură centrală, care sprijină instrumentul de căutare care permite interogarea simultană a registrelor naționale ale evidențelor poliției;

(c) un canal de comunicații securizat între infrastructura centrală, statele membre și Europol.

*Articolul 43*

**Utilizarea EPRIS**

(1) În scopul efectuării de căutări în registrele naționale ale evidențelor poliției prin intermediul EPRIS, se utilizează cel puțin două dintre următoarele seturi de date:

(a) prenumele;

(b) numele;

(c) data nașterii.

(2) În cazul în care sunt disponibile, se pot utiliza, de asemenea, următoarele seturi de date:

(a) pseudonimul sau pseudonimele și numele utilizat sau numele utilizate anterior;

(b) cetățenia sau cetățeniile;

(c) țara nașterii;

(d) genul.

(3) Datele menționate la alineatul (1) literele (a) și (b) și la alineatul (2) litera (a), trebuie să fie pseudonimizate.

*Articolul 44*

**Procedură**

(1) Atunci când statele membre sau Europol solicită o interogare, transmit datele menționate la articolul 43.

EPRIS transmite cererea de interogare către registrele naționale ale evidențelor poliției din statele membre cu datele transmise de statul membru solicitant sau Europol și în conformitate cu prezentul regulament.

(2) La primirea solicitării de interogare din partea EPRIS, fiecare stat membru solicitat lansează, în mod automatizat și fără întârziere, o interogare în registrul său național de evidențe ale poliției.

(3) Toate concordanțele rezultate în urma interogărilor menționate la alineatul (1) în registrele de evidențe ale poliției ale fiecărui stat membru solicitat sunt trimise înapoi în mod automatizat către EPRIS.

(4) Lista concordanțelor este returnată statului membru solicitant sau Europol de către EPRIS, în mod automatizat. Lista concordanțelor precizează calitatea concordanței și statul membru sau statele membre ale căror registre de evidențe ale poliției conțin date care au condus la concordanța sau la concordanțele respective.

(5) La primirea listei de concordanțe, statul membru solicitant decide cu privire la concordanțele pentru care este necesară o acțiune ulterioară și trimite, prin intermediul SIENA, statului membru solicitat sau statelor membre solicitate o solicitare motivată de acțiune ulterioară cuprinzând datele menționate la articolele 25 și 27, precum și eventuale informații suplimentare relevante. Statul membru solicitat sau statele membre solicitate prelucrează aceste solicitări fără întârziere pentru a decide dacă partajează datele stocate în baza lor de date.

(6) Comisia adoptă acte de punere în aplicare prin care precizează procedura tehnică pentru efectuarea de către EPRIS a interogării registrelor de evidențe ale poliției statelor membre, precum și formatul răspunsurilor și numărul maxim al acestora. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).

*Articolul 45*

**Păstrarea înregistrărilor**

(1) Fiecare stat membru participant și Europol păstrează înregistrări ale tuturor operațiunilor de prelucrare de date efectuate în EPRIS. În aceste înregistrări se includ următoarele informații:

(a) dacă un stat membru sau Europol a lansat solicitarea de interogare; dacă un stat membru a lansat solicitarea de interogare, se indică statul membru în cauză;

(b) data și ora solicitării;

(c) data și ora răspunsului;

(d) bazele de date naționale către care a fost trimisă o solicitare de interogare;

(e) bazele de date naționale care au oferit un răspuns.

(2) Fiecare stat membru participant păstrează înregistrări ale interogărilor efectuate de personalul autorităților sale competente autorizat în mod corespunzător să utilizeze EPRIS. Europol păstrează înregistrări ale solicitărilor de interogări pe care le efectuează personalul său autorizat în mod corespunzător.

(3) Înregistrările menționate la alineatele (1) și (2) pot fi folosite numai pentru colectarea de statistici și pentru monitorizarea protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, precum și pentru asigurarea securității și integrității datelor. Respectivele înregistrări se protejează prin măsuri corespunzătoare împotriva accesului neautorizat și se șterg după o perioadă de trei ani de la data la care au fost create. Dacă înregistrările sunt însă necesare pentru desfășurarea unor proceduri de monitorizare deja inițiate, acestea se șterg în momentul în care nu mai sunt necesare pentru procedurile de monitorizare.

(4) În scopul monitorizării protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, operatorii de date au acces la înregistrări pentru automonitorizarea menționată la articolul 55.

*Articolul 46*

**Proceduri de notificare în cazul imposibilității tehnice de a utiliza EPRIS**

(1) În cazul în care este imposibil din punct de vedere tehnic să se utilizeze EPRIS pentru a efectua interogări în unul sau mai multe registre naționale de evidențe ale poliției din cauza unei defecțiuni a infrastructurii Europol, Europol notifică acest lucru statelor membre în mod automatizat. Europol ia măsuri fără întârziere pentru a soluționa imposibilitatea tehnică de a utiliza EPRIS.

(2) În cazul în care este imposibil din punct de vedere tehnic să se utilizeze EPRIS pentru a efectua interogări în unul sau mai multe registre de evidențe ale poliției din cauza unei defecțiuni a infrastructurii naționale dintr-un stat membru, statul membru respectiv notifică acest lucru celorlalte state membre, Comisiei și Europol în mod automatizat. Statele membre iau măsuri fără întârziere pentru a soluționa imposibilitatea tehnică de a utiliza EPRIS.

*CAPITOLUL 4*

***Schimbul de date în urma unei concordanțe***

*Articolul 47*

**Schimbul de date de bază**

(1) Un set de date de bază se returnează prin router în termen de 48 de ore de la îndeplinirea cumulativă a condițiilor următoare:

(a) procedurile menționate la articolul 6, 11 sau 20 indică o concordanță între datele utilizate pentru căutare și datele stocate în baza de date a statului membru solicitat sau a statelor membre solicitate;

(b) concordanța menționată la litera (a) de la prezentul alineat a fost confirmată manual de către un membru calificat din statul membru solicitant astfel cum se menționează la articolul 6 alineatul (6), articolul 11 alineatul (2) și articolul 20 alineatul (2) sau, în cazul profilurilor ADN menționate la articolul 6 alineatul (7), de către statul membru solicitat;

(c) a fost transmisă o descriere a faptelor și a fost indicată infracțiunea subiacentă, utilizând tabelul comun al categoriilor de infracțiuni prevăzut într-un act de punere în aplicare care urmează să fie adoptat în temeiul articolului 11b alineatul (1) litera (a) din Decizia-cadru 2009/315/JAI, de către statul membru solicitant sau, în cazul profilurilor ADN menționate la articolul 6 alineatul (7), de către statul membru solicitat, pentru a evalua proporționalitatea cererii, inclusiv gravitatea infracțiunii pentru care a fost efectuată o căutare, în conformitate cu dreptul intern al statului membru care furnizează setul de date de bază.

(2) Atunci când, în temeiul dreptului său intern, un stat membru poate transmite un set de date de bază numai după obținerea unei autorizații judiciare, statul membru respectiv se poate abate de la termenele stabilite la alineatul (1) în măsura în care acest lucru este necesar pentru obținerea unei astfel de autorizații.

(3) Setul de date de bază menționat la alineatul (1) de la prezentul articol se returnează de către statul membru solicitat sau, în cazul profilurilor ADN menționate la articolul 6 alineatul (7), de către statul membru solicitant.

(4) În cazul în care concordanța confirmată se referă la datele identificate ale unei persoane, setul de date de bază menționat la alineatul (1) conține următoarele date, în măsura în care sunt disponibile:

(a) prenumele;

(b) numele de familie;

(c) pseudonimul sau pseudonimele și numele utilizat sau numele utilizate anterior;

(d) data nașterii;

(e) cetățenia sau cetățeniile;

(f) locul și țara nașterii;

(g) genul;

(h) data la care și locul unde au fost obținute datele biometrice;

(i) infracțiunea pentru care au fost obținute datele biometrice;

(j) numărul cauzei penale;

(k) autoritatea competentă responsabilă de cauza penală.

(5) În cazul în care concordanța confirmată se referă la date neidentificate sau urme, setul de date de bază menționat la alineatul (1) conține următoarele date, în măsura în care sunt disponibile:

(a) data la care și locul unde au fost obținute datele biometrice;

(b) infracțiunea pentru care au fost obținute datele biometrice;

(c) numărul cauzei penale;

(d) autoritatea competentă responsabilă de cauza penală.

(6) Returnarea datelor de bază de către statul membru solicitat sau, în cazul specific al profilurilor ADN menționate la articolul 6 alineatul (7), de către statul membru solicitant face obiectul unei decizii luate de un factor uman.

*CAPITOLUL 5*

***Europol***

*Articolul 48*

**Accesul statelor membre la datele biometrice furnizate de țări terțe și stocate de Europol**

(1) În conformitate cu Regulamentul (UE) 2016/794, statele membre au acces la datele biometrice puse la dispoziția Europol de către țările terțe în sensul articolului 18 alineatul (2) literele (a), (b) și (c) din Regulamentul (UE) 2016/794 și pot efectua căutări prin intermediul routerului.

(2) În cazul în care o căutare, astfel cum este menționată la alineatul (1), conduce la o concordanță între datele utilizate pentru căutare și datele furnizate de țări terțe și stocate de Europol, acțiunea ulterioară are loc în conformitate cu Regulamentul (UE) 2016/794.

*Articolul 49*

**Accesul Europol la datele stocate în bazele de date ale statelor membre, utilizând datele furnizate de țări terțe**

(1) Atunci când este necesar pentru realizarea obiectivelor stabilite la articolul 3 din Regulamentul (UE) 2016/794 și în conformitate cu respectivul regulament și cu prezentul regulament, Europol are acces la datele stocate de statele membre în bazele lor de date naționale și la registrele de evidențe ale poliției.

(2) Interogările efectuate de Europol utilizând date biometrice drept criteriu de căutare se efectuează utilizând routerul.

(3) Interogările efectuate de Europol utilizând date privind înmatricularea vehiculelor drept criteriu de căutare se efectuează utilizând Eucaris.

(4) Interogările efectuate de Europol utilizând date biografice ale suspecților și ale persoanelor condamnate în conformitate cu prevederile articolului 25 drept criteriu de căutare se efectuează utilizând EPRIS.

(5) Europol efectuează căutările pe baza datelor furnizate de țări terțe în conformitate cu alineatele (1)-(4) de la prezentul articol numai atunci când acest lucru este necesar pentru îndeplinirea atribuțiilor sale în sensul articolului 18 alineatul (2) literele (a) și (c) din Regulamentul (UE) 2016/794:

(6) În cazul în care procedurile menționate la articolele 6, 11 sau 20 indică o concordanță între datele utilizate pentru căutare și datele deținute în baza de date a statului membru solicitat sau a statelor membre solicitate, Europol informează numai statul membru implicat sau statele membre implicate.

Statul membru solicitat decide dacă returnează prin router un set de date de bază în termen de 48 de ore de la îndeplinirea cumulativă a condițiilor următoare:

(a) concordanța menționată la primul paragraf a fost confirmată manual de către un membru calificat al personalului Europol;

(b) a fost transmisă de către Europol o descriere a faptelor și a fost indicată infracțiunea subiacentă, utilizând tabelul comun al categoriilor de infracțiuni prevăzut într-un act de punere în aplicare care urmează să fie adoptat în temeiul articolului 11b alineatul (1) litera (a) din Decizia-cadru 2009/315/JAI, pentru a evalua proporționalitatea cererii, inclusiv gravitatea infracțiunii pentru care a fost efectuată o căutare, în conformitate cu dreptul intern al statului membru care furnizează setul de date de bază;

(c) a fost comunicat numele țării terțe care a furnizat datele;

Atunci când, în temeiul dreptului său intern, un stat membru poate transmite un set de date de bază numai după obținerea unei autorizații judiciare, statul membru respectiv se poate abate de la termenele stabilite la al doilea paragraf în măsura în care acest lucru este necesar pentru obținerea unei astfel de autorizații.

În cazul în care concordanța confirmată se referă la datele identificate ale unei persoane, setul de date de bază menționat la al doilea paragraf conține următoarele date, în măsura în care sunt disponibile:

(a) prenumele;

(b) numele de familie;

(c) pseudonimul sau pseudonimele și numele utilizat sau numele utilizate anterior;

(d) data nașterii;

(e) cetățenia sau cetățeniile;

(f) locul și țara nașterii;

(g) genul;

(h) data la care și locul unde au fost obținute datele biometrice;

(i) infracțiunea pentru care au fost obținute datele biometrice;

(j) numărul cauzei penale;

(k) autoritatea competentă responsabilă de cauza penală.

În cazul în care concordanța confirmată se referă la date neidentificate sau urme, setul de date de bază menționat la al doilea paragraf conține următoarele date, în măsura în care sunt disponibile:

(a) data la care și locul unde au fost obținute datele biometrice;

(b) infracțiunea pentru care au fost obținute datele biometrice;

(c) numărul cauzei penale;

(d) autoritatea competentă responsabilă de cauza penală.

Returnarea datelor de bază de către statul membru solicitat face obiectul unei decizii luate de un factor uman.

(7) Utilizarea de către Europol a informațiilor obținute în urma unei interogări efectuate în conformitate cu prezentul articol și a schimbului unui set de date de bază în conformitate cu alineatul (6) este condiționată de acordul statului membru în a cărui bază de date s-a obținut concordanța. Dacă statul membru permite utilizarea informațiilor respective, gestionarea acestora de către Europol intră sub incidența Regulamentului (UE) 2016/794.

*CAPITOLUL 6*

***Protecția datelor***

*Articolul 50*

**Scopul prelucrării datelor**

(1) Prelucrarea datelor cu caracter personal primite de către un stat membru sau de către Europol este permisă numai în scopurile pentru care datele au fost transmise de statul membru care a furnizat datele în conformitate cu prezentul regulament. Prelucrarea în alte scopuri este permisă numai cu autorizarea prealabilă a statului membru care a furnizat datele.

(2) Prelucrarea datelor furnizate de către un stat membru sau Europol în temeiul articolului 6, 11, 16, 20 sau 26 este permisă doar dacă este necesară în scopul:

(a) de a stabili dacă între profilurile ADN, datele dactiloscopice, datele privind înmatricularea vehiculelor, imaginile faciale sau evidențele poliției comparate există concordanțe;

(b) de a face schimb de un set de date de bază în conformitate cu articolul 47;

(c) de a pregăti și a depune o cerere formulată de organele de poliție sau judiciare în vederea acordării de asistență juridică, dacă s-a obținut o concordanță între date;

(d) de a păstra înregistrări astfel cum se prevede la articolele 18, 40 și 45.

(3) Datele primite de un stat membru sau de Europol se șterg imediat după răspunsurile automatizate la căutări, cu excepția cazului în care este necesară o prelucrare suplimentară în scopurile menționate la alineatul (2) sau o asemenea prelucrare este autorizată în conformitate cu alineatul (1).

(4) Înainte de a-și conecta bazele de date naționale la router sau la EPRIS, statele membre efectuează o evaluare a impactului asupra protecției datelor, astfel cum se menționează la articolul 27 din Directiva (UE) 2016/680, și, după caz, consultă autoritatea de supraveghere astfel cum se prevede la articolul 28 din directiva respectivă. Autoritatea de supraveghere poate face uz de oricare dintre competențele care îi revin în temeiul articolului 47 din directiva respectivă, în conformitate cu articolul 28 alineatul (5) din directiva respectivă.

*Articolul 51*

**Exactitatea, relevanța și păstrarea datelor**

(1) Statele membre și Europol asigură exactitatea și relevanța datelor cu caracter personal care sunt prelucrate în temeiul prezentului regulament. În cazul în care un stat membru sau Europol constată că au fost furnizate date care sunt incorecte sau nu mai sunt actuale sau date care nu ar fi trebuit furnizate, acesta notifică acest lucru statului membru care a primit datele sau Europol fără întârzieri nejustificate. Toate statele membre în cauză sau Europol corectează sau șterg datele în consecință, fără întârzieri nejustificate. În cazul în care statul membru care a primit datele sau Europol are motive să creadă că datele furnizate sunt incorecte sau ar trebui șterse, acesta informează statul membru care a furnizat datele fără întârzieri nejustificate.

(2) Statele membre și Europol instituie măsuri adecvate pentru actualizarea datelor relevante în sensul prezentului regulament.

(3) În cazul în care o persoană vizată a contestat exactitatea datelor aflate în posesia unui stat membru sau a Europol, dacă exactitatea nu poate fi stabilită în mod fiabil de către statul membru în cauză sau Europol și dacă persoana vizată solicită acest lucru, datele în cauză sunt marcate cu un marcaj. În cazul în care există un astfel de marcaj, statele membre sau Europol îl pot elimina numai cu permisiunea persoanei vizate sau pe baza unei decizii a instanței competente sau a autorității de supraveghere sau a Autorității Europene pentru Protecția Datelor, după caz.

(4) Datele cu caracter personal care nu ar fi trebuit să fie furnizate sau primite se șterg. Datele care sunt legal furnizate și primite se șterg:

(a) dacă nu sunt sau nu mai sunt necesare pentru scopul pentru care au fost furnizate;

(b) după expirarea termenului maxim de păstrare a datelor prevăzut de dreptul intern al statului membru care a furnizat datele, dacă statul membru respectiv a informat statul membru care a primit datele sau Europol cu privire la acest termen maxim la momentul furnizării datelor; sau

(c) după expirarea perioadei maxime de păstrare a datelor prevăzute în Regulamentul (UE) 2016/794.

În cazul în care există motive să se creadă că ștergerea datelor ar aduce atingere intereselor persoanei vizate, se restricționează prelucrarea datelor, în loc ca acestea să fie șterse. În cazul în care s-a restricționat prelucrarea datelor, acestea se prelucrează doar în scopul care a împiedicat ștergerea lor.

*Articolul 52*

**Persoana împuternicită de operatorul de date**

(1) eu-LISA este persoana împuternicită de operator în înțelesul articolului 3 punctul 12 din Regulamentul (UE) 2018/1725 pentru prelucrarea datelor cu caracter personal prin intermediul routerului.

(2) Europol este persoana împuternicită de operator în înțelesul articolului 3 punctul 12 din Regulamentul (UE) 2018/1725 pentru prelucrarea datelor cu caracter personal prin intermediul EPRIS.

*Articolul 53*

**Securitatea prelucrărilor de date**

(1) Autoritățile competente ale statelor membre, eu-LISA și Europol asigură securitatea prelucrării datelor cu caracter personal în temeiul prezentului regulament. Autoritățile competente ale statelor membre, eu-LISA și Europol cooperează în ceea ce privește atribuțiile legate de securitate.

(2) Fără a aduce atingere articolului 33 din Regulamentul (UE) 2018/1725 și articolului 32 din Regulamentul (UE) 2016/794, eu-LISA și Europol iau măsurile necesare pentru a asigura securitatea routerului și, respectiv, a EPRIS, precum și a infrastructurii de comunicații aferente acestora.

(3) eu-LISA adoptă măsurile necesare cu privire la router, iar Europol adoptă măsurile necesare cu privire la EPRIS, în următoarele scopuri:

(a) de a proteja fizic datele, inclusiv prin elaborarea de planuri de urgență pentru protejarea infrastructurii critice;

(b) de a interzice accesul persoanelor neautorizate la echipamentele și instalațiile de prelucrare a datelor;

(c) de a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a suporturilor de date;

(d) de a împiedica introducerea neautorizată de date, precum și orice inspectare, modificare sau ștergere neautorizată a datelor cu caracter personal înregistrate;

(e) de a împiedica prelucrarea neautorizată de date, precum și orice copiere, modificare sau ștergere neautorizată a datelor;

(f) de a împiedica utilizarea sistemelor de prelucrare automată a datelor de către persoane neautorizate prin utilizarea echipamentelor de comunicare de date;

(g) de a se asigura, prin utilizarea exclusivă a unor nume de utilizator individuale și a unor coduri de acces confidențiale, că persoanele autorizate să acceseze routerul sau EPRIS, după caz, au acces numai la datele care fac obiectul autorizației lor de acces;

(h) de a asigura posibilitatea de a verifica și de a stabili care sunt organismele cărora le pot fi furnizate datele cu caracter personal prin utilizarea echipamentelor de comunicare de date;

(i) de a asigura posibilitatea de a verifica și de a stabili ce date au fost prelucrate în router sau EPRIS, după caz, și în ce moment, de către cine și în ce scop au fost prelucrate;

(j) de a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transmiterii acestora către sau din router sau EPRIS, după caz, sau în timpul transportului suporturilor de date, în special prin intermediul unor tehnici de criptare corespunzătoare;

(k) de a asigura că, în cazul unei întreruperi, sistemele instalate pot fi readuse la funcționarea normală;

(l) de a asigura fiabilitatea prin garantarea faptului că este raportată în mod adecvat orice deficiență în funcționarea routerului sau a EPRIS, după caz;

(m) de a monitoriza eficacitatea măsurilor de securitate prevăzute la prezentul alineat și de a lua măsurile organizatorice necesare referitoare la monitorizarea internă, astfel încât să se asigure respectarea dispozițiilor prezentului regulament și să se evalueze măsurile de securitate respective în contextul noilor evoluții tehnologice.

Măsurile necesare menționate în primul paragraf includ un plan de securitate, un plan de asigurare a continuității activității și un plan de redresare în caz de dezastru.

*Articolul 54*

**Incidente de securitate**

(1) Orice eveniment care are sau poate avea un impact asupra securității routerului sau a EPRIS și care poate cauza daune sau pierderi ale datelor stocate în router sau EPRIS se consideră a fi un incident de securitate, în special în cazul în care este posibil să se fi accesat datele în mod neautorizat sau în cazul în care disponibilitatea, integritatea și confidențialitatea datelor au fost sau este posibil să fi fost compromise.

(2) În cazul unui incident de securitate privind routerul, eu-LISA și statele membre vizate sau, după caz, Europol cooperează între ele pentru a asigura un răspuns rapid, eficace și corespunzător.

(3) În cazul unui incident de securitate privind EPRIS, statele membre vizate și Europol cooperează între ele pentru a asigura un răspuns rapid, eficace și corespunzător.

(4) Statele membre notifică fără întârzieri nejustificate orice incident de securitate autorităților lor competente.

Fără a aduce atingere articolului 92 din Regulamentul (UE) 2018/1725, în cazul unui incident de securitate legat de infrastructura centrală a routerului, eu-LISA notifică Serviciul de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile Uniunii (CERT-UE) cu privire la amenințările cibernetice semnificative, la vulnerabilitățile semnificative și la incidentele semnificative, fără întârzieri nejustificate și, în orice caz, în termen de cel mult 24 de ore din momentul în care ia cunoștință de acestea. Detaliile tehnice operative și adecvate privind amenințările cibernetice, vulnerabilitățile și incidentele care permit detectarea proactivă, răspunsul la incidente sau măsurile de atenuare sunt comunicate către CERT-UE fără întârzieri nejustificate.

Fără a aduce atingere articolului 34 din Regulamentul (UE) 2016/794 și articolului 92 din Regulamentul (UE) 2018/1725, în cazul unui incident de securitate legat de infrastructura centrală a EPRIS, Europol notifică CERT-UE cu privire la amenințările cibernetice semnificative, la vulnerabilitățile semnificative și la incidentele semnificative, fără întârzieri nejustificate și, în orice caz, în termen de cel mult 24 de ore din momentul în care ia cunoștință de acestea. Detaliile tehnice operative și adecvate privind amenințările cibernetice, vulnerabilitățile și incidentele care permit detectarea proactivă, răspunsul la incidente sau măsurile de atenuare sunt comunicate către CERT-UE fără întârzieri nejustificate.

(5) Informațiile privind un incident de securitate care are sau poate avea un impact asupra funcționării routerului sau asupra disponibilității, integrității și confidențialității datelor sunt puse fără întârziere la dispoziția statelor membre și a Europol de către statele membre și agențiile Uniunii și se raportează în conformitate cu planul de gestionare a incidentelor care urmează să fie furnizat de eu-LISA.

(6) Informațiile privind un incident de securitate care are sau poate avea un impact asupra funcționării EPRIS sau asupra disponibilității, integrității și confidențialității datelor sunt puse fără întârziere la dispoziția statelor membre de către statele membre și agențiile Uniunii și se raportează în conformitate cu planul de gestionare a incidentelor care urmează să fie furnizat de Europol.

*Articolul 55*

**Automonitorizarea**

(1) Statele membre se asigură că fiecare autoritate care are dreptul de a utiliza cadrul Prüm II ia măsurile necesare pentru a monitoriza respectarea prezentului regulament și cooperează, dacă este cazul, cu autoritatea națională de supraveghere. Europol ia măsurile necesare pentru a monitoriza respectarea prezentului regulament și cooperează, dacă este necesar, cu Autoritatea Europeană pentru Protecția Datelor.

(2) Operatorii de date pun în aplicare măsurile necesare pentru a monitoriza efectiv respectarea dispozițiilor prezentului regulament pe parcursul prelucrării datelor, inclusiv prin verificarea frecventă a înregistrărilor menționate la articolele 18, 40 și 45. Aceștia cooperează, dacă este necesar și după caz, cu autoritățile de supraveghere sau cu Autoritatea Europeană pentru Protecția Datelor.

*Articolul 56*

**Sancțiuni**

Statele membre se asigură că orice utilizare abuzivă a datelor și orice prelucrare sau schimb de date care încalcă prezentul regulament sunt sancționate în conformitate cu dreptul intern. Sancțiunile prevăzute trebuie să fie efective, proporționale și cu efect de descurajare.

*Articolul 57*

**Răspunderea**

Dacă orice nerespectare de către un stat membru sau, la efectuarea de interogări în conformitate cu articolul 49, de către Europol a obligațiilor care îi revin în temeiul prezentului regulament provoacă prejudicii routerului sau EPRIS, răspunderea aparține statului membru respectiv sau Europol, cu excepția cazului în care eu-LISA, Europol sau un alt stat membru căruia îi revin obligații în temeiul prezentului regulament nu a luat măsuri rezonabile pentru a preveni producerea prejudiciului sau pentru a reduce la minimum impactul acestuia.

*Articolul 58*

**Auditurile efectuate de Autoritatea Europeană pentru Protecția Datelor**

(1) Autoritatea Europeană pentru Protecția Datelor garantează că cel puțin o dată la patru ani se realizează un audit al operațiunilor de prelucrare a datelor cu caracter personal desfășurate de eu-LISA și de Europol, în sensul prezentului regulament, în conformitate cu standardele internaționale de audit relevante. Un raport al acestui audit se trimite Parlamentului European, Consiliului, Comisiei, statelor membre și agenției în cauză a Uniunii. eu-LISA și Europol au posibilitatea de a formula observații înainte de adoptarea rapoartelor.

(2) eu-LISA și Europol pun la dispoziția Autorității Europene pentru Protecția Datelor informațiile solicitate de aceasta și oferă Autorității Europene pentru Protecția Datelor acces la toate documentele solicitate de aceasta și la înregistrările lor menționate la articolele 40 și 45, precum și la toate sediile proprii, în orice moment. Prezentul alineat nu aduce atingere competențelor Autorității Europene pentru Protecția Datelor în temeiul articolului 58 din Regulamentul (UE) 2018/1725 și, în ceea ce privește Europol, în temeiul articolului 43 alineatul (3) din Regulamentul (UE) 2016/794.

*Articolul 59*

**Cooperarea dintre autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor**

(1) Autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor, fiecare acționând în limitele competențelor sale, cooperează activ în cadrul responsabilităților lor pentru a asigura o supraveghere coordonată a aplicării prezentului regulament, în special dacă Autoritatea Europeană pentru Protecția Datelor sau o autoritate de supraveghere identifică discrepanțe majore între practicile statelor membre sau transferuri potențial ilegale efectuate prin canalele de comunicare ale cadrului Prüm II.

(2) În cazurile menționate la alineatul (1) de la prezentul articol, se asigură o supraveghere coordonată în conformitate cu articolul 62 din Regulamentul (UE) 2018/1725.

(3) La doi ani de la intrarea în funcțiune a routerului și a EPRIS și, ulterior, din doi în doi ani, Comitetul european pentru protecția datelor transmite Parlamentului European, Consiliului, Comisiei, eu-LISA și Europol un raport privind activitățile sale în temeiul prezentului articol. Raportul respectiv include un capitol despre fiecare stat membru, elaborat de autoritatea de supraveghere a statului membru respectiv.

*Articolul 60*

**Transferul de date cu caracter personal către țări terțe și organizații internaționale**

Un stat membru transferă datele cu caracter personal pe care le-a obținut în temeiul prezentului regulament către o țară terță sau o organizație internațională numai în conformitate cu capitolul V din Directiva (UE) 2016/680 și cu condiția ca statul membru solicitat să fi acordat autorizația înainte de transfer.

Europol transferă datele cu caracter personal pe care le-a obținut în temeiul prezentului regulament către o țară terță sau o organizație internațională numai dacă au fost îndeplinite condițiile prevăzute la articolul 25 din Regulamentul (UE) 2016/794 și cu condiția ca statul membru solicitat să fi acordat autorizația înainte de transfer.

*Articolul 61*

**Relația cu alte acte juridice privind protecția datelor**

Orice prelucrare a datelor cu caracter personal în sensul prezentului regulament se efectuează în conformitate cu prezentul capitol și cu Directiva (UE) 2016/680 sau Regulamentul (UE) 2018/1725, Regulamentul (UE) 2016/794 sau Regulamentul (UE) 2016/679, după caz.

*CAPITOLUL 7*

***Responsabilități***

*Articolul 62*

**Responsabilitatea pentru diligența necesară**

Statele membre și Europol exercită diligența necesară atunci când evaluează dacă schimbul automatizat de date se încadrează în obiectivul cadrului Prüm II prevăzut la articolul 2 și dacă acesta respectă condițiile prevăzute la articolul respectiv, în special în ceea ce privește respectarea drepturilor fundamentale.

*Articolul 63*

**Formarea**

Personalul autorizat al autorităților competente ale statelor membre, al autorităților de supraveghere și al Europol beneficiază, după caz, de resurse și formare adecvate, inclusiv în ceea ce privește protecția datelor și examinarea exactă a concordanțelor, pentru a îndeplini sarcinile prevăzute în prezentul regulament.

*Articolul 64*

**Responsabilitățile statelor membre**

(1) Fiecare stat membru este responsabil pentru:

(a) conectarea la infrastructura routerului;

(b) integrarea sistemelor și infrastructurii sale naționale existente cu routerul;

(c) organizarea, gestionarea, exploatarea și întreținerea infrastructurii naționale existente și conectarea acesteia la router;

(d) conectarea la infrastructura EPRIS;

(e) integrarea sistemelor și infrastructurii sale naționale existente cu EPRIS;

(f) organizarea, gestionarea, exploatarea și întreținerea infrastructurii sale naționale existente și conectarea acesteia la EPRIS;

(g) gestionarea accesului și modalitățile de accesare a routerului de către personalul autorizat în mod corespunzător al autorităților sale competente, în conformitate cu prezentul regulament, precum și crearea și actualizarea periodică a unei liste a membrilor personalului respectiv și a profilurilor acestora;

(h) gestionarea accesului și modalitățile de accesare a EPRIS de către personalul autorizat în mod corespunzător al autorităților sale competente, în conformitate cu prezentul regulament, precum și crearea și actualizarea periodică a unei liste a membrilor personalului respectiv și a profilurilor acestora;

(i) gestionarea accesului și modalitățile de accesare a Eucaris de către personalul autorizat în mod corespunzător al autorităților sale competente, în conformitate cu prezentul regulament, precum și crearea și actualizarea periodică a unei liste a membrilor personalului respectiv și a profilurilor acestora;

(j) confirmarea manuală de către membri ai personalului calificat a unei concordanțe, astfel cum se menționează la articolul 6 alineatele (6) și (7), articolul 11 alineatul (2) și articolul 20 alineatul (2);

(k) asigurarea disponibilității datelor necesare pentru schimbul de date în conformitate cu articolele 5, 10, 16, 19 și 25;

(l) schimbul de informații în conformitate cu articolele 6, 11, 16, 20 și 26;

(m) corectarea, actualizarea sau ștergerea oricăror date primite de la un stat membru solicitat în termen de 48 de ore de la notificarea statului membru solicitat cu privire la faptul că datele transmise au fost incorecte, nu mai sunt actualizate sau au fost transmise ilegal;

(n) conformitatea cu cerințele de calitate a datelor stabilite în prezentul regulament.

(2) Fiecare stat membru este responsabil pentru conectarea autorităților sale competente la router, la EPRIS și la Eucaris.

*Articolul 65*

**Responsabilitățile Europol**

(1) Europol este responsabil pentru gestionarea accesului și modalitățile de accesare a routerului, a EPRIS și a Eucaris de către personalul său autorizat în mod corespunzător, în conformitate cu prezentul regulament.

(2) Europol este responsabil pentru prelucrarea interogărilor în datele Europol de către router. Europol își adaptează sistemele de informații în consecință.

(3) Europol este responsabil pentru orice adaptări tehnice ale infrastructurii Europol necesare pentru stabilirea conectării la router și la Eucaris.

(4) Fără a aduce atingere căutărilor efectuate de Europol în temeiul articolului 49, Europol nu are acces la niciuna dintre datele cu caracter personal prelucrate prin intermediul EPRIS.

(5) Europol este responsabil pentru dezvoltarea EPRIS în cooperare cu statele membre. EPRIS oferă funcționalitățile prevăzute la articolele 42-46.

Europol este responsabil pentru gestionarea tehnică a EPRIS. Gestionarea tehnică a EPRIS constă în toate sarcinile și soluțiile tehnice necesare pentru a menține funcționarea infrastructurii centrale a EPRIS și furnizarea neîntreruptă de servicii statelor membre, 24 de ore pe zi, 7 zile pe săptămână, în conformitate cu prezentul regulament. Gestionarea tehnică include lucrările de întreținere și dezvoltările tehnice necesare pentru a se asigura funcțiile EPRIS la un nivel satisfăcător de calitate tehnică, în special în ceea ce privește timpul de răspuns pentru transmiterea de solicitări către bazele de date naționale în conformitate cu specificațiile tehnice.

(6) Europol asigură formarea pentru utilizarea tehnică a EPRIS.

(7) Europol este responsabil pentru procedurile prevăzute la articolele 48 și 49.

*Articolul 66*

**Responsabilitățile eu-LISA în etapa de concepere și dezvoltare a routerului**

(1) eu-LISA se asigură că infrastructura centrală a routerului este exploatată în conformitate cu prezentul regulament.

(2) Routerul este găzduit de eu-LISA în amplasamentele sale tehnice și asigură funcționalitățile prevăzute în prezentul regulament, în conformitate cu condițiile de securitate, disponibilitate, calitate și performanță menționate la articolul 67 alineatul (1).

(3) Agenția eu-LISA este responsabilă pentru dezvoltarea routerului și pentru orice adaptări tehnice necesare pentru funcționarea routerului.

(4) eu-LISA nu are acces la niciuna dintre datele cu caracter personal prelucrate prin router.

(5) eu-LISA definește modul în care este concepută arhitectura fizică a routerului, inclusiv a infrastructurii sale de comunicații securizată, precum și specificațiile tehnice și evoluția acesteia în ceea ce privește infrastructura centrală și infrastructura de comunicații securizată. Consiliul de administrație al eu-LISA aprobă modul de concepere, sub rezerva unui aviz favorabil din partea Comisiei. De asemenea, eu-LISA pune în aplicare orice adaptare necesară a componentelor de interoperabilitate care rezultă din instituirea routerului, astfel cum se prevede în prezentul regulament.

(6) eu-LISA dezvoltă și implementează routerul cât mai curând posibil după adoptarea de către Comisie a măsurilor prevăzute la articolul 37 alineatul (6). Dezvoltarea respectivă constă în elaborarea și implementarea specificațiilor tehnice, efectuarea de teste și gestionarea și coordonarea generală a proiectului.

(7) În cursul etapei de concepere și dezvoltare, Consiliul de administrație al programului menționat la articolul 54 din Regulamentul (UE) 2019/817 și la articolul 54 din Regulamentul (UE) 2019/818 se reunește periodic. Acesta asigură gestionarea adecvată a etapei de concepere și dezvoltare a routerului.

Consiliul de administrație al programului prezintă lunar Consiliului de administrație al eu-LISA rapoarte scrise privind evoluția proiectului. Consiliul de administrație al programului nu are competențe decizionale și nu dispune de un mandat pentru a-i reprezenta pe membrii Consiliului de administrație al eu-LISA.

Grupul consultativ pentru interoperabilitate menționat la articolul 78 se reunește cu regularitate până la începerea funcționării routerului. După fiecare reuniune, acesta prezintă un raport Consiliului de administrație al programului. Grupul consultativ furnizează expertiza tehnică necesară în sprijinul atribuțiilor care revin Consiliului de administrație al programului și monitorizează stadiul de pregătire al statelor membre.

*Articolul 67*

**Responsabilitățile eu-LISA după începerea funcționării routerului**

(1) După punerea în funcțiune a routerului, eu-LISA este responsabilă pentru gestionarea tehnică a infrastructurii centrale a routerului, inclusiv pentru întreținerea acestuia și pentru dezvoltările tehnologice. În cooperare cu statele membre, aceasta se asigură că se utilizează cea mai bună tehnologie disponibilă, sub rezerva unei analize cost-beneficiu. eu-LISA este, de asemenea, responsabilă pentru gestionarea tehnică a infrastructurii de comunicații necesare.

Gestionarea tehnică a routerului cuprinde toate sarcinile și soluțiile tehnice necesare pentru a menține funcționarea routerului și furnizarea neîntreruptă de servicii statelor membre și Europol 24 de ore pe zi, 7 zile pe săptămână, în conformitate cu prezentul regulament. Gestionarea tehnică include lucrările de întreținere și dezvoltările tehnice necesare pentru a se asigura funcționarea routerului la un nivel satisfăcător de calitate tehnică, în special în ceea ce privește disponibilitatea și timpul de răspuns pentru transmiterea de solicitări către bazele de date naționale și către datele Europol în conformitate cu specificațiile tehnice.

Routerul este dezvoltat și gestionat astfel încât să se asigure accesul rapid, eficient și controlat, o disponibilitate deplină și neîntreruptă, precum și un timp de răspuns în conformitate cu nevoile operaționale ale autorităților competente ale statelor membre și ale Europol.

(2) Fără a aduce atingere articolului 17 din Statutul funcționarilor Uniunii Europene prevăzut în Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului ([18]), eu-LISA aplică norme corespunzătoare privind secretul profesional sau alte responsabilități echivalente de confidențialitate membrilor personalului său care trebuie să lucreze cu date stocate în router. Această obligație se aplică și după ce persoanele respective au încetat să mai ocupe o anumită funcție sau după ce și-au încetat activitatea.

eu-LISA nu are acces la niciuna dintre datele cu caracter personal prelucrate prin router.

(3) eu-LISA îndeplinește sarcini legate de asigurarea formării privind utilizarea tehnică a routerului.

*CAPITOLUL 8*

***Modificarea altor instrumente existente***

*Articolul 68*

**Modificarea Deciziilor 2008/615/JAI și 2008/616/JAI**

(1) În Decizia 2008/615/JAI, articolul 1 litera (a), articolele 2-6 și secțiunile 2 și 3 din capitolul 2 se înlocuiesc în ceea ce privește statele membre care au obligații în temeiul prezentului regulament de la data aplicării dispozițiilor prezentului regulament referitoare la router prevăzute la articolul 75 alineatul (1). Prin urmare, articolul 1 litera (a), articolele 2-6 și secțiunile 2 și 3 din capitolul 2 din Decizia 2008/615/JAI se elimină de la data aplicării dispozițiilor prezentului regulament referitoare la router prevăzute la articolul 75 alineatul (1).

(2) În Decizia 2008/616/JAI, capitolele 2-5 și articolele 18, 20 și 21 se înlocuiesc în ceea ce privește statele membre care au obligații în temeiul prezentului regulament de la data aplicării dispozițiilor prezentului regulament referitoare la router prevăzute la articolul 75 alineatul (1). Prin urmare, capitolele 2-5 și articolele 18, 20 și 21 din Decizia 2008/616/JAI se elimină de la data aplicării dispozițiilor prezentului regulament referitoare la router prevăzute la articolul 75 alineatul (1).

*Articolul 69*

**Modificarea Regulamentului (UE) 2018/1726**

Regulamentul (UE) 2018/1726 se modifică după cum urmează:

1. Se introduce următorul articol:

„*Articolul 8d*

**Atribuții legate de routerul Prüm II**

([18]) JO L 56, 4.3.1968, p. 1.

În legătură cu routerul Prüm II, agenția îndeplinește atribuțiile care îi sunt conferite prin Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului (*).

_____

(*) 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) (JO L, 2024/982, 5.4.2024, ELI: http://data.europa.eu/eli/reg/2024/982/oj)."

2. La articolul 17 alineatul (3), al doilea paragraf se înlocuiește cu următorul text:

„Atribuțiile legate de dezvoltarea și gestionarea operațională menționate la articolul 1 alineatele (4) și (5), la articolele 3-8 și la articolele 8d, 9 și 11 sunt îndeplinite la amplasamentul tehnic de la Strasbourg, Franța."

3. Articolul 19 alineatul (1) se modifică după cum urmează:

(a) se introduce următoarea literă:

„(eeb) adoptă rapoarte privind stadiul dezvoltării routerului Prüm II în temeiul articolului 80 alineatul (2) din Regulamentul (UE) 2024/982;";

(b) litera (ff) se înlocuiește cu următorul text:

„(ff) adoptă rapoarte privind funcționarea tehnică a următoarelor:

(i) a SIS în temeiul articolului 60 alineatul (7) din Regulamentul (UE) 2018/1861 al Parlamentului European și al Consiliului (*) și al articolului 74 alineatul (8) din Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului (**);

(ii) a VIS în temeiul articolului 50 alineatul (3) din Regulamentul (CE) nr. 767/2008 și al articolului 17 alineatul (3) din Decizia 2008/633/JAI;

(iii) a SEE în temeiul articolului 72 alineatul (4) din Regulamentul (UE) 2017/2226;

(iv) a ETIAS în temeiul articolului 92 alineatul (4) din Regulamentul (UE) 2018/1240;

(v) a ECRIS-TCN și a aplicației de referință a ECRIS în temeiul articolului 36 alineatul (8) din Regulamentul (UE) 2019/816;

(vi) a componentelor de interoperabilitate în temeiul articolului 78 alineatul (3) din Regulamentul (UE) 2019/817 și al articolului 74 alineatul (3) din Regulamentul (UE) 2019/818;

(vii) a sistemului e-CODEC în temeiul articolului 16 alineatul (1) din Regulamentul (UE) 2022/850;

(viii) a platformei de colaborare pentru JIT în temeiul articolului 26 alineatul (6) din Regulamentul (UE) 2023/969;

(ix) a routerului Prüm II în temeiul articolului 80 alineatul (5) din Regulamentul (UE) 2024/982;

_____

(*) Regulamentul (UE) 2018/1861 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Convenției de punere în aplicare a Acordului Schengen și de modificare și abrogare a Regulamentului (CE) nr. 1987/2006 (JO L 312, 7.12.2018, p. 14).

(**) Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală, de modificare și de abrogare a Deciziei 2007/533/JAI a Consiliului și de abrogare a Regulamentului (CE) nr. 1986/2006 al Parlamentului European și al Consiliului și a Deciziei 2010/261/UE a Comisiei (JO L 312, 7.12.2018, p. 56).";

(c) litera (hh) se înlocuiește cu următorul text:

„(hh) adoptă observații formale referitoare la rapoartele Autorității Europene pentru Protecția Datelor privind auditurile în temeiul articolului 56 alineatul (2) din Regulamentul (UE) 2018/1861, al articolului 42 alineatul (2) din Regulamentul (CE) nr. 767/2008, al articolului 31 alineatul (2) din Regulamentul (UE) nr. 603/2013, al articolului 56 alineatul (2) din Regulamentul (UE) 2017/2226, al articolului 67 din Regulamentul (UE) 2018/1240, al articolului 29 alineatul (2) din Regulamentul (UE) 2019/816, al articolului 52 din Regulamentul (UE) 2019/817 și Regulamentul (UE) 2019/818 și al articolului 58 alineatul (1) din Regulamentul (UE) 2024/982 și asigură luarea de măsuri corespunzătoare prin care să se dea curs recomandărilor formulate în cadrul auditurilor respective;".

*Articolul 70*

**Modificarea Regulamentului (UE) 2019/817**

La articolul 6 alineatul (2) din Regulamentul (UE) 2019/817 se adaugă următoarea literă:

„(d) o infrastructură de comunicații securizată între ESP și routerul instituit prin Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului (*).

_____

(*) 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) (JO L, 2024/982, 5.4.2024, ELI: http://data.europa.eu/eli/reg/2024/982/oj)."

*Articolul 71*

**Modificarea Regulamentului (UE) 2019/818**

Regulamentul (UE) 2019/818 se modifică după cum urmează:

1. La articolul 6 alineatul (2), se adaugă următoarea literă:

„(d) o infrastructură de comunicații securizată între ESP și routerul instituit prin Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului (*).

_____

(*) 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) (JO L, 2024/982, 5.4.2024, ELI: http://data.europa.eu/eli/reg/2024/982/oj)."

2. La articolul 39, alineatele (1) și (2) se înlocuiesc cu următorul text:

„(1) Se instituie un registru central de raportare și statistici (CRRS) în scopul de a susține obiectivele SIS, Eurodac și ECRIS-TCN, în conformitate cu instrumentele juridice respective care reglementează sistemele menționate, și de a furniza date statistice utilizabile între sisteme și rapoarte analitice în scopuri de elaborare a politicilor, operaționale și de asigurare a calității datelor. CRRS sprijină, de asemenea, obiectivele Regulamentului (UE) 2024/982.

(2) eu-LISA creează, implementează și găzduiește în amplasamentele sale tehnice CRRS care conține datele și statisticile menționate la articolul 74 din Regulamentul (UE) 2018/1862 și la articolul 32 din Regulamentul (UE) 2019/816 separate în mod logic pe sisteme de informații ale UE. De asemenea, eu-LISA colectează datele și statisticile de la routerul menționat la articolul 72 alineatul (1) din Regulamentul (UE) 2024/982. Accesul la CRRS se acordă printr-un acces controlat și securizat și cu profiluri de utilizator specifice, exclusiv în scopul întocmirii de rapoarte și statistici, autorităților menționate la articolul 74 din Regulamentul (UE) 2018/1862, la articolul 32 din Regulamentul (UE) 2019/816 și la articolul 72 alineatul (1) din Regulamentul (UE) 2024/982."

*CAPITOLUL 9*

***Dispoziții finale***

*Articolul 72*

**Raportare și statistici**

(1) Dacă este necesar, personalul autorizat în mod corespunzător din cadrul autorităților competente ale statelor membre, din cadrul Comisiei, al eu-LISA și al Europol are acces la următoarele date referitoare la router, exclusiv în scopul întocmirii de rapoarte și statistici:

(a) numărul de interogări pentru fiecare stat membru și numărul de interogări pentru Europol pe categorie de date;

(b) numărul de interogări în fiecare dintre bazele de date conectate;

(c) numărul de concordanțe cu baza de date a fiecărui stat membru pentru fiecare categorie de date;

(d) numărul de concordanțe cu datele Europol pentru fiecare categorie de date;

(e) numărul de concordanțe confirmate în cazul cărora au avut loc schimburi de date de bază;

(f) numărul de concordanțe confirmate în cazul cărora nu au avut loc schimburi de date de bază;

(g) numărul de interogări în registrul comun de date de identitate prin router; și

(h) numărul de concordanțe pe tip după cum urmează:

(i) date identificate (persoană) – date neidentificate (urme);

(ii) date neidentificate (urme) – date identificate (persoană);

(iii) date neidentificate (urme) – date neidentificate (urme);

(iv) date identificate (persoană) – date identificate (persoană).

Datele prevăzute la primul paragraf nu trebuie să permită identificarea persoanelor.

(2) Personalul autorizat în mod corespunzător din cadrul autorităților competente ale statelor membre, din cadrul Comisiei și al Europol are acces la următoarele date referitoare la Eucaris, exclusiv în scopul întocmirii de rapoarte și statistici:

(a) numărul de interogări pentru fiecare stat membru și numărul de interogări pentru Europol;

(b) numărul de interogări în fiecare dintre bazele de date conectate; și

(c) numărul de concordanțe cu baza de date a fiecărui stat membru.

Datele prevăzute la primul paragraf nu trebuie să permită identificarea persoanelor.

(3) Personalul autorizat în mod corespunzător din cadrul autorităților competente ale statelor membre, din cadrul Comisiei și al Europol are acces la următoarele date referitoare la EPRIS, exclusiv în scopul întocmirii de rapoarte și statistici:

(a) numărul de interogări pentru fiecare stat membru și numărul de interogări pentru Europol;

(b) numărul de interogări în fiecare dintre registrele conectate; și

(c) numărul de concordanțe cu baza de date a fiecărui stat membru.

Datele prevăzute la primul paragraf nu trebuie să permită identificarea persoanelor.

(4) eu-LISA stochează datele prevăzute la alineatul (1) de la prezentul articol în registrul central de raportare și statistici instituit prin articolul 39 din Regulamentul (UE) 2019/818. Europol stochează datele prevăzute la alineatul (3). Datele respective permit autorităților competente ale statelor membre, Comisiei, eu-LISA și Europol să obțină rapoarte și statistici adaptabile pentru a spori eficiența cooperării în materie de asigurare a respectării legii.

*Articolul 73*

**Costuri**

(1) Costurile aferente instituirii și funcționării routerului și a EPRIS sunt suportate din bugetul general al Uniunii.

(2) Costurile aferente integrării infrastructurii naționale existente și conexiunile acesteia cu routerul și EPRIS, precum și costurile suportate în legătură cu crearea bazelor de date naționale cu imagini faciale și a registrelor naționale ale evidențelor poliției pentru prevenirea, depistarea și investigarea infracțiunilor sunt suportate din bugetul general al Uniunii.

Sunt excluse următoarele costuri:

(a) costurile aferente birourilor de gestionare a proiectelor din statele membre (reuniuni, misiuni, spații de lucru);

(b) costurile aferente găzduirii sistemelor informatice naționale (spații, implementare, energie electrică, răcire);

(c) costurile aferente exploatării sistemelor informatice naționale (operatori și contracte de asistență);

(d) costurile aferente conceperii, dezvoltării, implementării, exploatării și întreținerii rețelelor naționale de comunicații.

(3) Fiecare stat membru suportă costurile care decurg din administrarea, utilizarea și întreținerea Eucaris.

(4) Fiecare stat membru suportă costurile care decurg din administrarea, utilizarea și întreținerea conexiunilor sale cu routerul și EPRIS.

*Articolul 74*

**Notificări**

(1) Statele membre notifică agenției eu-LISA autoritățile competente menționate la articolul 36. Respectivele autorități pot utiliza routerul sau pot avea acces la acesta.

(2) eu-LISA notifică Comisiei finalizarea cu succes a testării menționate la articolul 75 alineatul (1) litera (b).

(3) Europol notifică Comisiei finalizarea cu succes a testării menționate la articolul 75 alineatul (3) litera (b).

(4) Fiecare stat membru transmite celorlalte state membre, Comisiei, eu-LISA și Europol conținutul bazelor sale naționale de date ADN și condițiile pentru căutările automatizate cărora li se aplică articolele 5 și 6.

(5) Fiecare stat membru informează celelalte state membre, Comisia, eu-LISA și Europol cu privire la conținutul bazelor sale de date dactiloscopice naționale și la condițiile pentru căutările automatizate cărora li se aplică articolele 10 și 11.

(6) Fiecare stat membru informează celelalte state membre, Comisia, eu-LISA și Europol cu privire la conținutul bazelor sale de date naționale privind imaginile faciale și la condițiile pentru căutările automatizate cărora li se aplică articolele 19 și 20.

(7) Statele membre care participă la schimburile automatizate de evidențe ale poliției în temeiul articolelor 25 și 26 transmit celorlalte state membre, Comisiei și Europol conținutul registrelor lor naționale de evidențe ale poliției și al bazelor naționale de date utilizate pentru stabilirea registrelor respective și condițiile pentru căutările automatizate.

(8) Statele membre notifică Comisiei, eu-LISA și Europol punctul lor de contact național desemnat în temeiul articolului 30. Comisia întocmește o listă a punctelor de contact naționale care i-au fost notificate și o pune la dispoziția tuturor statelor membre.

*Articolul 75*

**Începerea funcționării**

(1) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care statele membre și Europol pot începe să utilizeze routerul, după îndeplinirea următoarelor condiții:

(a) măsurile prevăzute la articolul 5 alineatul (3), la articolul 8 alineatele (2) și (3), la articolul 13 alineatele (2) și (3), la articolul 17 alineatul (3), la articolul 22 alineatele (2) și (3), la articolul 31 și la articolul 37 alineatul (6) au fost adoptate;

(b) eu-LISA a notificat finalizarea cu succes a unei testări complete a routerului, pe care a efectuat-o în cooperare cu autoritățile competente ale statelor membre și cu Europol.

Comisia stabilește, prin intermediul actului de punere în aplicare menționat în primul paragraf, data de la care statele membre și Europol urmează să înceapă să utilizeze routerul. Respectiva dată este la un an de la data stabilită în conformitate cu primul paragraf.

Comisia poate amâna cu cel mult un an data de la care statele membre și Europol urmează să înceapă să utilizeze routerul, în cazul în care o evaluare a implementării routerului a indicat că o astfel de amânare este necesară.

(2) Statele membre asigură, la doi ani de la începerea funcționării routerului, disponibilitatea imaginilor faciale, astfel cum se menționează la articolul 19, în scopul căutării automatizate a imaginilor faciale, astfel cum se menționează la articolul 20.

(3) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care statele membre și Europol urmează să înceapă să utilizeze EPRIS, după îndeplinirea următoarelor condiții:

(a) măsurile prevăzute la articolul 44 alineatul (6) au fost adoptate;

(b) Europol a notificat finalizarea cu succes a unei testări complete a EPRIS, pe care a efectuat-o în cooperare cu autoritățile competente ale statelor membre.

(4) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care Europol urmează să pună la dispoziția statelor membre datele biometrice provenite din țări terțe, în conformitate cu articolul 48, după îndeplinirea următoarelor condiții:

(a) routerul este în funcțiune;

(b) Europol a notificat finalizarea cu succes a unei testări complete a conexiunii sale cu routerul, pe care a efectuat-o în cooperare cu autoritățile competente ale statelor membre și cu eu-LISA.

(5) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care Europol urmează să aibă acces la datele stocate în bazele de date ale statelor membre în conformitate cu articolul 49, după îndeplinirea următoarelor condiții:

(a) routerul este în funcțiune;

(b) Europol a notificat finalizarea cu succes a unei testări complete a conexiunii sale cu routerul, pe care a efectuat-o în cooperare cu autoritățile competente ale statelor membre și cu eu-LISA.

(6) Actele de punere în aplicare menționate la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 77 alineatul (2).

*Articolul 76*

**Dispoziții tranzitorii și derogări**

(1) Statele membre și agențiile Uniunii încep să aplice articolele 19-22, articolul 47 și articolul 49 alineatul (6) de la data stabilită în conformitate cu articolul 75 alineatul (1) primul paragraf, cu excepția statelor membre care nu au început să utilizeze routerul.

(2) Statele membre și agențiile Uniunii încep să aplice articolele 25-28 și articolul 49 alineatul (4) de la data stabilită în conformitate cu articolul 75 alineatul (3).

(3) Statele membre și agențiile Uniunii încep să aplice articolul 48 de la data stabilită în conformitate cu articolul 75 alineatul (4).

(4) Statele membre și agențiile Uniunii încep să aplice articolul 49 alineatele (1), (2), (3), (5) și (7) de la data stabilită în conformitate cu articolul 75 alineatul (5).

*Articolul 77*

**Procedura comitetului**

(1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011. În cazul în care comitetul nu emite un aviz, Comisia nu adoptă proiectul de act de punere în aplicare și se aplică articolul 5 alineatul (4) al treilea paragraf din Regulamentul (UE) nr. 182/2011.

*Articolul 78*

**Grupul consultativ pentru interoperabilitate**

Responsabilitățile Grupului consultativ pentru interoperabilitate instituit prin articolul 75 din Regulamentul (UE) 2019/817 și articolul 71 din Regulamentul (UE) 2019/818 se extind pentru a include routerul. Grupul consultativ pentru interoperabilitate furnizează eu-LISA cunoștințele de specialitate legate de router, în special în contextul pregătirii programului său de lucru anual și al raportului său anual de activitate.

*Articolul 79*

**Manual practic**

Comisia, în strânsă cooperare cu statele membre, cu eu-LISA, cu Europol și cu Agenția pentru Drepturi Fundamentale a Uniunii Europene, pune la dispoziție un manual practic pentru punerea în aplicare și gestionarea prezentului regulament. Manualul practic furnizează orientări, recomandări și bune practici cu caracter tehnic și operațional. Comisia adoptă manualul practic sub forma unei recomandări înainte de începerea funcționării routerului și a EPRIS. Comisia actualizează manualul practic periodic și acolo unde este necesar.

*Articolul 80*

**Monitorizare și evaluare**

(1) eu-LISA se asigură că există proceduri pentru a monitoriza dezvoltarea routerului din perspectiva obiectivelor legate de planificare și costuri și pentru a monitoriza funcționarea sa din perspectiva obiectivelor legate de realizările tehnice, de raportul cost-eficiență, de securitate și de calitatea serviciilor.

Europol se asigură că există proceduri pentru a monitoriza dezvoltarea EPRIS din perspectiva obiectivelor legate de planificare și costuri și pentru a monitoriza funcționarea sa din perspectiva obiectivelor legate de realizările tehnice, de raportul cost-eficiență, de securitate și de calitatea serviciilor.

(2) Până la 26 aprilie 2025 și, ulterior, în fiecare an pe durata fazei de dezvoltare a routerului, eu-LISA prezintă Parlamentului European și Consiliului un raport privind stadiul dezvoltării routerului. Respectivele rapoarte conțin informații detaliate cu privire la costurile ocazionate, precum și informații despre riscurile care ar putea avea un impact asupra costurilor totale care urmează să fie suportate din bugetul general al Uniunii în temeiul articolului 73.

După încheierea etapei de dezvoltare a routerului, eu-LISA transmite Parlamentului European și Consiliului un raport în care explică în detaliu modul în care au fost îndeplinite obiectivele, în special cele referitoare la planificare și costuri, și în care se justifică eventualele abateri.

(3) Până la 26 aprilie 2025 și, ulterior, în fiecare an în cursul etapei de dezvoltare a EPRIS, Europol prezintă Parlamentului European și Consiliului un raport privind stadiul dezvoltării EPRIS. Respectivele rapoarte conțin informații detaliate cu privire la costurile ocazionate, precum și informații despre riscurile care ar putea avea un impact asupra costurilor totale care urmează să fie suportate din bugetul general al Uniunii în temeiul articolului 73.

După încheierea etapei de dezvoltare a EPRIS, Europol transmite Parlamentului European și Consiliului un raport în care explică în detaliu modul în care au fost îndeplinite obiectivele, în special cele referitoare la planificare și costuri, și în care se justifică eventualele abateri.

(4) În vederea întreținerii tehnice, eu-LISA are acces la informațiile necesare referitoare la operațiunile de prelucrare a datelor efectuate în router. În vederea întreținerii tehnice, Europol are acces la informațiile necesare referitoare la operațiunile de prelucrare a datelor efectuate în EPRIS.

(5) După doi ani de la începerea funcționării routerului și, ulterior, o dată la doi ani, eu-LISA prezintă Parlamentului European, Consiliului și Comisiei un raport privind funcționarea tehnică a routerului, inclusiv în ceea ce privește securitatea routerului.

(6) După doi ani de la începerea funcționării EPRIS și, ulterior, o dată la doi ani, Europol prezintă Parlamentului European, Consiliului și Comisiei un raport privind funcționarea tehnică a EPRIS, inclusiv în ceea ce privește securitatea EPRIS.

(7) După trei ani de la punerea în funcțiune a routerului și a EPRIS, astfel cum se prevede la articolul 75 și, ulterior, o dată la patru ani, Comisia prezintă un raport de evaluare globală a cadrului Prüm II.

După un an de la punerea în funcțiune a routerului și, ulterior, o dată la doi ani, Comisia prezintă un raport de evaluare globală a utilizării imaginilor faciale în temeiul prezentului regulament.

Rapoartele menționate la primul și al doilea paragraf includ următoarele:

(a) o analiză a aplicării prezentului regulament, inclusiv utilizarea lui de către fiecare stat membru și Europol;

(b) o examinare a rezultatelor obținute în raport cu obiectivele prezentului regulament și a impactului său asupra drepturilor fundamentale;

(c) impactul, eficacitatea și eficiența activității cadrului Prüm II și ale practicilor sale de lucru având în vedere obiectivele, mandatul și atribuțiile sale;

(d) o evaluare a gradului de securitate al cadrului Prüm II.

Comisia transmite rapoartele respective Parlamentului European, Consiliului, Autorității Europene pentru Protecția Datelor și Agenției pentru Drepturi Fundamentale a Uniunii Europene.

(8) În rapoartele menționate la alineatul (7) primul paragraf, Comisia acordă o atenție deosebită următoarelor noi categorii de date: imaginile faciale și evidențele poliției. Comisia include în astfel de rapoarte utilizarea de către fiecare stat membru și Europol a respectivelor noi categorii de date și impactul, eficacitatea și eficiența acestora. În rapoartele menționate la alineatul (7) al doilea paragraf, Comisia acordă o atenție deosebită riscului de concordanțe false și calității datelor.

(9) Statele membre și Europol furnizează eu-LISA și Comisiei informațiile necesare pentru elaborarea rapoartelor menționate la alineatele (2) și (5). Respectivele informații nu trebuie să pericliteze metodele de lucru și nici să dezvăluie sursele, membrii personalului sau investigațiile autorităților competente din statele membre.

(10) Statele membre transmit Comisiei și Europol informațiile necesare pentru elaborarea rapoartelor prevăzute la alineatele (3) și (6). Respectivele informații nu trebuie să pericliteze metodele de lucru și nici să dezvăluie sursele, membrii personalului sau investigațiile autorităților competente din statele membre.

(11) Fără a aduce atingere cerințelor în materie de confidențialitate, statele membre, eu-LISA și Europol furnizează Comisiei informațiile necesare pentru realizarea rapoartelor menționate la alineatul (7). De asemenea, statele membre transmit Comisiei numărul de concordanțe confirmate în baza de date a fiecărui stat membru pentru fiecare categorie și pentru fiecare tip de date. Respectivele informații nu trebuie să pericliteze metodele de lucru și nici să dezvăluie sursele, membrii personalului sau investigațiile autorităților competente din statele membre.

*Articolul 81*

**Intrarea în vigoare și aplicabilitatea**

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în statele membre în conformitate cu tratatele.

Adoptat la Strasbourg, 13 martie 2024.

| *Pentru Parlamentul European* | *Pentru Consiliu* |
|---|---|
| *Președinta* | *Președintele* |
| R. METSOLA | H. LAHBIB |