



COMISIA
EUROPEANĂ

Bruxelles, 8.12.2021
COM(2021) 784 final

2021/0410 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

**privind schimbul automatizat de date în scopul cooperării polițienești („Prüm II”), de
modificare a Deciziilor 2008/615/JAI și 2008/616/JAI ale Consiliului și a Regulamentelor
(UE) 2018/1726, 2019/817 și 2019/818 ale Parlamentului European și ale Consiliului**

{SEC(2021) 421 final} - {SWD(2021) 378 final} - {SWD(2021) 379 final}

EXPUNERE DE MOTIVE

CONTEXTUL PROPUNERII

• Motivele propunerii

În întreaga Europă, criminalitatea subminează securitatea și bunăstarea cetățenilor UE. Autoritățile de aplicare a legii au nevoie de instrumente solide și performante pentru a combate criminalitatea în mod eficace. Cooperarea și schimbul de informații sunt cele mai puternice mijloace de combatere a criminalității și de îndeplinire a actului de justiție¹. În 2021, s-a constatat că peste 70 % din grupurile infracționale organizate erau prezente în mai mult de trei state membre². Chiar și în cazul infracțiunilor care par să fi fost comise strict la nivel local, pot exista legături cu alte locuri din Europa în care același autor a săvârșit fapte penale. În mod similar, adeseori legăturile dintre criminalitatea presupusă a fi locală și structuri și operațiuni de criminalitate organizată nu sunt evidente. Prin urmare, pentru a putea combate în mod eficace criminalitatea, autoritățile de aplicare a legii trebuie să fie în măsură să facă schimb de date în timp util. UE a pus deja la dispoziția autorităților de aplicare a legii o serie de instrumente pentru a facilita schimbul de informații, care s-au dovedit esențiale pentru descoperirea activităților și rețelelor infracționale³, dar există încă lacune care trebuie remediate în ceea ce privește informațiile. În plus, având în vedere că datele sunt stocate separat în diferite sisteme informatice naționale, precum și, la nivelul UE, în sisteme informatice la scară largă, este necesar să se asigure că sistemele pot comunica între ele.

Într-un spațiu fără controale la frontierele interne („spațiul Schengen”), există încă frontiere și obstacole atunci când autoritățile de aplicare a legii⁴ trebuie să facă schimb de date, ceea ce creează unghiuri moarte și lacune de care profită numeroși infractori și teroriști care acționează în mai multe state membre. Prezenta inițiativă, împreună cu propunerea de directivă – adoptată în paralel – privind schimbul de informații între autoritățile de aplicare a legii din statele membre⁵, vizează consolidarea schimbului de informații între statele membre și, prin urmare, punerea la dispoziția autorităților de aplicare a legii din UE a unor instrumente îmbunătățite de combatere a criminalității și a terorismului⁶.

De peste zece ani, cadrul Prüm facilitează schimbul de informații între autoritățile de aplicare a legii de la nivelul UE. Deciziile Prüm⁷, adoptate în 2008 cu scopul de a sprijini cooperarea polițienească și judiciară transfrontalieră în materie penală, prevăd schimbul automatizat de date specifice (profiluri ADN, amprente digitale și date privind înmatricularea vehiculelor) între autoritățile responsabile cu prevenirea, depistarea și cercetarea infracțiunilor. Cadrul Prüm contribuie cu succes la combaterea criminalității și a terorismului în UE, dar există încă lacune în domeniul schimbului de informații și, prin urmare, pot fi aduse îmbunătățiri suplimentare.

¹ A se vedea Strategia UE privind uniunea securității din 2020 – COM(2020) 605 final (24.7.2020).

² Evaluarea amenințării pe care o reprezintă formele grave de criminalitate și criminalitatea organizată în UE 2021.

³ Strategia UE de combatere a criminalității organizate 2021-2025, COM(2021) 170 final (14.4.2021).

⁴ Cum ar fi modul în care sunt transmise anumite categorii de date, canalul utilizat pentru aceste schimburi, termenele aplicabile etc.

⁵ [Referință].

⁶ Comunicarea privind Strategia pentru realizarea unui spațiu Schengen pe deplin funcțional și rezilient, COM(2021) 277 final (2.6.2021).

⁷ Decizia 2008/615/JAI a Consiliului privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere și Decizia 2008/616/JAI a Consiliului privind punerea în aplicare a Deciziei 2008/615/JAI. Deciziile Consiliului se bazează pe Convenția de la Prüm din 2005.

Concluziile Consiliului privind punerea în aplicare a Deciziilor Prüm la zece ani de la adoptarea acestora au subliniat importanța căutării și comparării automatizate a profilurilor ADN, a datelor dactiloscopice și a datelor privind înmatricularea vehiculelor pentru combaterea terorismului și a criminalității transfrontaliere. De asemenea, Consiliul a invitat Comisia să ia în considerare revizuirea Deciziilor Prüm în vederea extinderii domeniului lor de aplicare și a actualizării cerințelor tehnice și juridice necesare⁸.

Prüm II se bazează pe cadrul Prüm existent, pe care îl consolidează și modernizează, permițând interoperabilitatea cu alte sisteme de informații ale UE. Astfel se va asigura posibilitatea ca toate datele relevante care sunt disponibile pentru autoritățile de aplicare a legii dintr-un stat membru să fie utilizate și de autoritățile de aplicare a legii din alte state membre. De asemenea, se va asigura posibilitatea ca Europol să ofere sprijin statelor membre în contextul cadrului Prüm. Prezenta inițiativă prevede crearea unei noi arhitecturi, care să permită un efectuare de schimburi de date mai ușor și mai rapid între statele membre și care să asigure un nivel ridicat de protecție a drepturilor fundamentale.

- **Obiectivele propunerii**

Obiectivul general al prezentei propunerii rezultă din obiectivul înscris în tratat de a contribui la securitatea internă a Uniunii Europene. Printre măsurile prevăzute în acest sens se numără colectarea, stocarea, prelucrarea și analiza informațiilor în domeniu, precum și schimbul de informații⁹. Prin urmare, obiectivul general al acestui instrument este de a îmbunătăți, a eficientiza și a facilita schimbul de informații în scopul prevenirii, al depistării și al cercetării infracțiunilor și a actelor de terorism între autoritățile de aplicare a legii din statele membre, dar și cu Europol ca centru de informații în materie penală al UE.

Obiectivele de politică specifice ale acestei propunerii sunt:

- (a) furnizarea unei soluții tehnice pentru ca autoritățile de aplicare a legii din UE să poată face schimburi automatizate eficiente de date, astfel încât acestea să aibă acces la datele relevante care sunt disponibile în baza de date națională a unui alt stat membru;
- (b) asigurarea disponibilității – pentru toate autoritățile competente de aplicare a legii – a unor date mai relevante (din punctul de vedere al categoriilor de date) din bazele de date naționale ale altor state membre;
- (c) asigurarea disponibilității – pentru autoritățile de aplicare a legii – a datelor relevante (din punctul de vedere al surselor de date) din bazele de date ale Europol;
- (d) asigurarea – pentru autoritățile de aplicare a legii – a unui acces eficient la datele efective corespunzătoare unui rezultat pozitiv care sunt disponibile în baza de date națională a unui alt stat membru.

- **Coerența cu dispozițiile existente în domeniul de politică vizat**

Recenta Strategie privind spațiul Schengen¹⁰ a anunțat o serie de măsuri de intensificare a cooperării polițienești și a schimbului de informații între autoritățile de aplicare a legii pentru a consolida securitatea într-un spațiu intrinsec interdependent, fără frontiere interne. Împreună cu propunerea de directivă privind schimbul de informații între autoritățile de aplicare a legii din statele membre,

⁸ Concluziile Consiliului privind punerea în aplicare a „DECIZIILOR PRÜM” la zece ani de la adoptarea lor (documentul 11227/18), <https://data.consilium.europa.eu/doc/document/ST-11227-2018-INIT/ro/pdf>.

⁹ Articolul 87 alineatul (2) litera (a) din TFUE.

¹⁰ Comunicare a Comisiei către Parlamentul European și Consiliu „Strategie pentru realizarea unui spațiu Schengen pe deplin funcțional și rezilient”, COM(2021) 277 final (2.6.2021).

prezenta propunere contribuie la obiectivele acestei strategii prin asigurarea faptului că autoritățile de aplicare a legii dintr-un stat membru au acces la aceleași informații care sunt disponibile pentru colegii lor din alt stat membru.

Propunerea se înscrie în peisajul mai larg al sistemelor informatice la scară largă ale UE, care s-a dezvoltat substanțial de la adoptarea cadrului Prüm. Acesta include cele trei sisteme centrale de informații ale UE care sunt în funcțiune: Sistemul de informații Schengen (SIS), Sistemul de informații privind vizele (VIS) și sistemul Eurodac¹¹. În plus, alte trei sisteme sunt în prezent în etapa de dezvoltare: Sistemul de intrare/ieșire (EES), Sistemul european de informații și de autorizare privind călătoriile (ETIAS) și sistemul centralizat de identificare a statelor membre în care există informații privind condamnările resortisanților țărilor terțe și ale apatrizilor (sistemul ECRIS-TCN)¹². Toate aceste sisteme actuale și viitoare sunt conectate prin intermediul cadrului de interoperabilitate pentru sistemele de informații ale UE¹³ de gestionare a securității, a frontierelor și a migrației, care a fost adoptat în 2019 și care este în prezent în curs de implementare. Revizuirile incluse în prezenta propunere vizează alinierea cadrului Prüm la cadrul de interoperabilitate, în special în ceea ce privește schimbul de date și arhitectura generală oferită de interoperabilitatea sistemelor de informații ale UE. Acest lucru ar asigura accesul rapid și controlat la informațiile de care au nevoie agenții de aplicare a legii pentru a-și îndeplini atribuțiile și pentru care au drepturi de acces.

SIS conține deja semnalări privind persoane dispărute și permite efectuarea de căutări pe baza amprentelor digitale. SIS este un sistem de informații operative centralizat de tip „rezultat pozitiv/negativ”, accesibil direct unui număr mare de utilizatori finali din prima linie; sistemul conține semnalări și oferă un răspuns imediat la fața locului, existând acțiuni care trebuie întreprinse în legătură cu subiectul semnalării. SIS este utilizat în principal pentru controalele polițienești, la frontieră și vamale, precum și de către autoritățile responsabile în domeniul vizelor și al migrației în cadrul procedurilor și verificărilor de rutină.

În schimb, cadrul Prüm nu are nicio componentă centrală/bază de date la nivelul UE și este utilizat doar în anchetele penale. Acesta permite altor state membre să acceseze subseturi de date depersonalizate din bazele de date naționale privind ADN-ul și amprente digitale ale tuturor statelor membre conectate. Accesul este acordat numai punctelor de contact naționale. Rezultatul pozitiv/negativ este furnizat în câteva secunde sau minute, dar poate dura săptămâni sau chiar luni pentru a primi datele cu caracter personal corespunzătoare referitoare la rezultatul pozitiv obținut.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

• Temeiul juridic

Temeiul juridic al prezentei propuneri este reprezentat de următoarele dispoziții din Tratatul privind funcționarea Uniunii Europene (TFUE): articolul 16 alineatul (2), articolul 87 alineatul (2) litera (a) și articolul 88 alineatul (2).

¹¹ SIS ajută autoritățile competente din UE să mențină securitatea internă în absența verificărilor la frontierele interne, iar VIS permite statelor Schengen să facă schimb de date privind vizele. Sistemul Eurodac reprezintă o bază de date dactiloscopice a UE în materie de azil, care permite statelor membre să compare amprente digitale ale solicitanților de azil pentru a vedea dacă aceștia au solicitat anterior azil sau au intrat în UE în mod neregular printr-un alt stat membru.

¹² EES și ETIAS vor consolida controalele de securitate ale călătorilor scutiți de obligația de a deține viză, permițând efectuarea de verificări prealabile în materie de migrație ilegală și de securitate. Sistemul ECRIS-TCN va remedia lacunele identificate în ceea ce privește schimbul de informații între statele membre cu privire la resortisanții țărilor terțe condamnați.

¹³Regulamentul (UE) 2019/817 și Regulamentul (UE) 2019/818.

În temeiul articolului 16 alineatul (2), Uniunea are competența de a adopta măsuri referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii, precum și de către statele membre în exercitarea activităților care fac parte din domeniul de aplicare a dreptului Uniunii, precum și normele privind libera circulație a acestor date. În temeiul articolului 87 alineatul (2) litera (a), Uniunea are competența de a adopta măsuri privind colectarea, stocarea, prelucrarea și analizarea informațiilor în domeniu, precum și schimbul de informații pentru a asigura cooperarea polițienească între autoritățile competente ale statelor membre, inclusiv serviciile de poliție, serviciile vamale și alte servicii specializate de aplicare a legii în domeniul prevenirii sau al depistării și al cercetării infracțiunilor. În temeiul articolului 88 alineatul (2), Parlamentul European și Consiliul pot stabili structura, funcționarea, domeniul de acțiune și atribuțiile Europol.

- **Subsidiaritatea**

Îmbunătățirea schimbului de informații între poliție și autoritățile de aplicare a legii din cadrul UE nu poate fi realizată într-o măsură suficientă de către statele membre în mod izolat, din cauza caracterului transfrontalier al combaterii criminalității și al problemelor de securitate. Statele membre trebuie să se bazeze unele pe altele în această privință.

Prin intermediul mai multor proiecte de punere în aplicare la nivelul UE¹⁴, statele membre au încercat să ia măsuri pentru a remedia deficiențele actualului cadru Prüm¹⁵. În pofida tuturor acestor acțiuni, multe dintre deficiențe au rămas la fel cum au fost descrise în raportul din 2012 privind punerea în aplicare a Deciziei Prüm¹⁶. Acest lucru demonstrează necesitatea unei acțiuni la nivelul UE, deoarece s-a dovedit că limitările actualului cadru Prüm nu se pot remedia doar prin măsuri puse în aplicare la nivel național, de către statele membre.

În plus, existența unor norme, standarde și cerințe comune la nivelul UE facilitează schimburile de informații, asigurând în același timp compatibilitatea între diferitele sisteme naționale. Acest lucru permite, la rândul său, un anumit nivel de automatizare a fluxurilor de lucru pentru schimbul de informații, care degrevează agenții de aplicare a legii de activitățile manuale care utilizează intensiv forța de muncă.

- **Proportionalitatea**

Astfel cum se explică în detaliu în evaluarea impactului care însoțește prezenta propunere de regulament, opțiunile în materie de politică sunt considerate proporționale, deoarece acestea nu depășesc ceea ce este necesar pentru atingerea obiectivelor identificate.

Propunerea prevede crearea unor **routeri centrale** (routerul Prüm II și EPRIS), care ar acționa fiecare ca punct de legătură între statele membre. Aceasta este o abordare hibridă între o soluție descentralizată și una centralizată fără stocarea de date la nivel central. Abordarea presupune ca bazele de date

¹⁴ De exemplu, proiectul privind Echipa de competență mobilă (*Mobile Competence Team – MCT*) (2011-2014) a fost inițiat de Germania și finanțat prin programul Comisiei „Prevenirea și combaterea criminalității” (ISEC). MCT a avut scopul de a furniza cunoștințe de specialitate și sprijin statelor membre ale UE care nu erau încă operaționale pentru schimbul de date ADN și de date dactiloscopice.

¹⁵ Prin intermediul unui proiect condus de Finlanda, statele membre au analizat procedurile naționale aplicate în urma obținerii unui rezultat pozitiv. Pe baza concluziilor acestui proiect s-au formulat recomandări cu privire la o serie de bune practici neobligatorii pentru eficientizarea schimbului de informații în urma obținerii unui rezultat pozitiv la nivelul UE (a se vedea documentul 14310/2/16 REV2, care nu este public).

În plus, Europol a sprijinit în perioada 2012-2013 elaborarea unor formulare standardizate care să fie utilizate pentru schimbul ulterior de informații, independent de canalul de comunicare utilizat (a se vedea documentul 9383/13 pentru mai multe informații). Totuși, nu se cunoaște în ce măsură punctele de contact naționale utilizează aceste formulare.

¹⁶ COM(2012) 732 final.

naționale din fiecare stat membru să se conecteze la routerul central în loc să se conecteze între ele. Routerile ar urma să servească drept brokeri de mesaje care transmit tranzacții de căutare și răspunsuri către sistemele naționale, fără a crea noi procese de date, fără a extinde drepturile de acces și fără a înlocui bazele de date naționale. Această abordare ar urma să garanteze accesul rapid și controlat al autorităților de aplicare a legii la informațiile de care au nevoie pentru a-și îndeplini atribuțiile, în conformitate cu drepturile lor de acces. Routerul ar urma să faciliteze punerea în aplicare de către statele membre a schimburilor de date actuale și viitoare în contextul cadrului Prüm.

Schimbul automatizat de categorii de date suplimentare, cum ar fi imaginile faciale și cazierele judiciare, este esențial pentru eficacitatea cercetărilor penale și pentru identificarea infractorilor. Introducerea acestor categorii de date suplimentare nu ar urma să ducă la stocarea de noi categorii de date, întrucât statele membre le colectează deja în temeiul dreptului intern și le stochează în bazele de date naționale. Schimbul de astfel de categorii noi de date ar urma să constituie o nouă prelucrare de date. Schimburile ar urma să fie însă limitate la ceea ce este necesar pentru atingerea scopului lor și să permită compararea datelor numai în situații individuale. Propunerea prevede, de asemenea, un set de garanții (de exemplu, schimbul de date complete numai în cazul în care există un rezultat pozitiv în urma unei interogări).

Prin această propunere, **Europol** va face parte integrantă din cadrul Prüm. Acest lucru va însemna, în primul rând, că statele membre vor putea să verifice în mod automat datele biometrice provenite din țări terțe și deținute de Europol. În al doilea rând, Europol va putea, de asemenea, să verifice datele provenite din țări terțe în bazele de date naționale ale statelor membre. Aceste două aspecte ale implicării Europol în noul cadru Prüm, în conformitate cu atribuțiile agenției astfel cum sunt prevăzute în Regulamentul (UE) 2016/794, ar urma să garanteze faptul că nu apar lacune în ceea ce privește datele primite de la țări terțe referitoare la criminalitatea gravă și la terorism. În cadrul unei societăți deschise aflate într-o lume globalizată, datele furnizate de țările terțe cu privire la infractori și teroriști sunt esențiale. Astfel s-ar facilita identificarea potențială a infractorilor cunoscuți de țările din afara UE, beneficiind în același timp de garanții solide în ceea ce privește protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor, stabilite în acordurile de cooperare ale Europol cu țările terțe.

Procesul revizuit de schimb de informații ca urmare a unui rezultat pozitiv ar urma să contribuie la securitatea internă a Uniunii Europene prin simplificarea și eficientizarea schimbului de informații în materie de asigurare a respectării legii. În comparație cu situația actuală, în care schimbul de informații în urma obținerii unui rezultat pozitiv este reglementat de legislația națională și, prin urmare, face obiectul unor norme și proceduri diferite, normele comune de armonizare a acestei a doua etapă a procesului Prüm ar urma să ofere predictibilitate tuturor utilizatorilor, deoarece ar ști toți ce date ar obține în această etapă. Schimbul de date ar urma să fie facilitat prin automatizare parțială, ceea ce înseamnă că intervenția umană ar fi în continuare necesară înainte ca un schimb cuprinzător de date să poată avea loc ulterior. Statele membre ar urma să păstreze proprietatea/controlul asupra datelor lor.

- **Alegerea instrumentului**

Se propune adoptarea unui regulament al Parlamentului European și al Consiliului. Legislația propusă se bazează pe un cadru existent de decizii ale Consiliului care contribuie la cooperarea transfrontalieră dintre statele membre ale UE în domeniul justiției și afacerilor interne¹⁷.

¹⁷ Decizia 2008/615/JAI a Consiliului privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere și Decizia 2008/616/JAI a Consiliului privind punerea în aplicare a Deciziei 2008/615/JAI.

Având în vedere necesitatea ca măsurile propuse să fie direct aplicabile și aplicate uniform în toate statele membre, precum și să îmbunătățească schimbul de informații, un regulament este, prin urmare, alegerea adecvată a instrumentului juridic.

3. REZULTATELE EVALUĂRILOR *EX-POST*, ALE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRII IMPACTULUI

• Evaluările *ex-post* ale legislației existente

În general, din evaluarea cadrului Prüm¹⁸ a reieșit că, pentru garantarea securității interne a UE și a siguranței cetățenilor săi, este capital să se poată efectua căutări și comparări ale datelor ADN, ale amprentelor digitale și ale datelor privind înmatricularea vehiculelor în bazele de date ale altor state membre în scopul prevenirii și al cercetării infracțiunilor. Evaluarea a demonstrat, de asemenea, că Deciziile Prüm au contribuit la stabilirea unor norme, standarde și cerințe comune la nivelul UE ce facilitează schimbul de informații și asigură compatibilitatea între diferitele sisteme naționale.

De la expirarea termenului de punere în aplicare a cadrului Prüm, în urmă cu zece ani, UE a adoptat însă o serie de alte măsuri privind facilitarea schimbului de informații între autoritățile de aplicare a legii¹⁹, printre care se numără și cadrul de interoperabilitate²⁰. În plus, dispozițiile privind specificațiile tehnice ale interogărilor, măsurile de securitate și comunicarea nu au fost actualizate de la adoptarea Deciziilor Prüm în 2008²¹. Unele dintre aceste norme sunt caduce, deoarece criminalistica și tehnologia în acest domeniu s-au dezvoltat în mod semnificativ în ultimul deceniu.

De asemenea, în urma evaluării s-a constatat că punerea în aplicare a Deciziilor Prüm a fost lentă în ultimii zece ani și că nu toate statele membre au luat măsurile necesare pentru punerea în aplicare a deciziilor²². În consecință, unele conexiuni bilaterale nu se pot realiza și nu se pot lansa căutări în bazele de date ale unor state membre. Evaluarea a indicat, de asemenea, că acțiunile ulterioare rezultatelor pozitive au loc în temeiul dreptului intern și, prin urmare, nu intră în domeniul de aplicare al Deciziilor Prüm. Diferențele dintre normele și procedurile naționale pot cauza, în mai multe situații, întâzieri semnificative în primirea de către autoritățile competente de informații în urma obținerii unui rezultat pozitiv. Această situație afectează funcționarea sistemului Prüm, precum și schimbul eficient de informații între statele membre prin reducerea posibilității de identificare a infractorilor și de depistare a legăturilor transfrontaliere dintre infracțiuni.

Constatările evaluării au fost utilizate în pregătirea evaluării impactului și a prezentei propuneri.

¹⁸ Anexa 4 la documentul de lucru de însoțire al serviciilor Comisiei [referința pentru evaluarea impactului sistemului Prüm].

¹⁹ Cum ar fi sistemul informațional Europol (EIS), sistemele de informații ale Interpolului și Sistemul de informații Schengen (SIS).

²⁰ 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; 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.

²¹ Cuprinse în Decizia 2008/616/JAI a Consiliului.

²² În 2016, Comisia a lansat proceduri de constatare a neîndeplinirii obligațiilor împotriva a cinci state membre. În octombrie 2021, două dintre aceste cazuri de constatare a neîndeplinirii obligațiilor erau încă deschise.

- **Consultările cu părțile interesate**

Pentru elaborarea prezentei propuneri s-au derulat consultări specifice cu părțile interesate vizate, inclusiv cu utilizatorii finali ai sistemului, și anume cu autoritățile statelor membre care utilizează schimbul automatizat de date Prüm, de la autoritățile de aplicare a legii și autoritățile judiciare, autoritățile naționale de înmatriculare a vehiculelor, până la custozii ai bazelor de date naționale și laboratoare criminalistice. Europol și eu-LISA au fost, de asemenea, consultate având în vedere expertiza lor și rolul potențial în noul cadru Prüm.

FRA, precum și organizațiile neguvernamentale precum EDRi (*European Digital Rights*) și organizațiile interguvernamentale (Eucaris – Sistemul de informații european privind vehiculele și permisele de conducere) au furnizat, de asemenea, informații prin prisma expertizei lor.

Activitățile de consultare desfășurate în contextul elaborării evaluării impactului care stă la baza prezentei propuneri au colectat feedback de la părțile interesate în diverse foruri. Aceste activități au inclus în special o evaluare inițială a impactului, o consultare publică și o serie de ateliere tehnice. A fost realizat un studiu de fezabilitate bazat pe cercetare documentară, interviuri cu experți în domeniu, chestionare și trei ateliere de experți. Studiul a examinat fezabilitatea îmbunătățirii schimbului de informații în temeiul Deciziilor Prüm.

Discuțiile periodice privind schimbul de informații în materie de asigurare a respectării legii și în special privind deciziile Prüm în cadrul Grupului de lucru DAPIX/IXIM²³ al Consiliului au contribuit, de asemenea, la pregătirea prezentei propuneri.

O **evaluare inițială a impactului** a fost publicată pentru a primi feedback în perioada august-octombrie 2020 și a primit în total șase contribuții²⁴.

O **consultare publică** anunțată pe site-ul Comisiei Europene s-a adresat publicului larg. Răspunsurile au confirmat faptul că actualul cadru Prüm este relevant pentru prevenirea și cercetarea infracțiunilor și a îmbunătățit schimbul de date între autoritățile de aplicare a legii din statele membre. Prin prevenirea necesității de a efectua interogări bilaterale în fiecare stat membru, schimbul automatizat de date în temeiul cadrului Prüm a contribuit, de asemenea, la creșterea eficienței. Răspunsurile au confirmat, de asemenea, coerența cadrului cu acțiunile UE și internaționale în acest domeniu și faptul că acesta are o valoare adăugată în comparație cu ceea ce ar putea realiza statele membre în domeniul schimbului de informații în materie de asigurare a respectării legii în absența cadrului Prüm. În ceea ce privește consolidarea cadrului actual, majoritatea respondenților au fost de acord că faptul că unele categorii de date nu sunt acoperite de cadru și, prin urmare, sunt partajate prin trimiterea de interogări manuale reprezintă o deficiență.

Serviciile Comisiei au organizat, de asemenea, o serie de **ateliere tehnice** informale specifice cu experți din statele membre și din țările asociate spațiului Schengen. Atelierele au avut ca scop reunirea utilizatorilor finali pentru un schimb de opinii cu privire la opțiunile avute în vedere și evaluate în vederea consolidării cadrului Prüm, din punct de vedere tehnic.

Evaluarea impactului care însoțește prezenta comunicare conține o descriere mai detaliată a consultării părților interesate (anexa 2).

²³ Grupul de lucru pentru protecția datelor al Consiliului (DAPIX) și, începând cu 1 ianuarie 2020, Grupul de lucru pentru schimbul de informații în domeniul JAI (IXIM).

²⁴ Evaluarea inițială a impactului și contribuțiile sunt disponibile [aici](#).

- **Evaluarea impactului**

Propunerea este susținută de o evaluare a impactului, prezentată în documentul de lucru însoțitor al serviciilor Comisiei [referința pentru evaluarea impactului sistemului Prüm]. Comitetul de control normativ a examinat proiectul de evaluare a impactului în cadrul reuniunii sale din 14 iulie 2021 și a emis un aviz favorabil la 16 iulie 2021.

Din evaluarea impactului a rezultat că:

- (1) Pentru a îndeplini obiectivul de a oferi o soluție tehnică pentru un schimb automatizat eficient de date, ar trebui să se aplice o soluție hibridă între o abordare descentralizată și o abordare centralizată fără stocarea datelor la nivel central.
- (2) Pentru a îndeplini obiectivul de a asigura disponibilitatea – pentru autoritățile de aplicare a legii – a unor date mai relevante (din punctul de vedere al categoriilor de date), ar trebui introdus schimbul de imagini faciale și de caziere judiciare.
- (3) Pentru a îndeplini obiectivul de a asigura disponibilitatea – pentru autoritățile de aplicare a legii – a datelor relevante din bazele de date ale Europol, ar trebui ca statele membre să poată verifica automat datele biometrice provenite din țări terțe disponibile la nivelul Europol, ca parte a cadrului Prüm. De asemenea, ar trebui ca Europol să poată verifica datele provenite din țări terțe în bazele de date naționale ale statelor membre.
- (4) Pentru a îndeplini obiectivul de a oferi un acces eficient la datele efective corespunzătoare unui rezultat pozitiv care sunt disponibile în baza de date națională a unui alt stat membru sau la nivelul Europol, ar trebui ca acțiunile ulterioare să fie reglementate la nivelul UE cu un schimb semiautomatizat de date reale care corespund unui răspuns pozitiv.

Impactul pozitiv major al prezentei propuneri va fi acela de a răspunde în mod eficace problemelor identificate și de a consolida actualul cadru Prüm cu capacități suplimentare specifice și puternice pentru a intensifica sprijinul acordat statelor membre în ceea ce privește consolidarea schimbului de informații având ca obiectiv final prevenirea și cercetarea infracțiunilor și a actelor de terorism, cu respectarea deplină a drepturilor fundamentale.

Beneficiarii finali ai tuturor opțiunilor preferate sunt cetățenii, care vor beneficia în mod direct și indirect de consolidarea luptei împotriva criminalității și de scăderea ratei criminalității. În ceea ce privește eficiența, principalii beneficiari sunt autoritățile naționale de aplicare a legii.

Impactul financiar și economic imediat al propunerii va necesita investiții atât la nivelul UE, cât și la nivelul statelor membre. Costurile de investiții estimate se preconizează că vor fi compensate prin beneficii și economii, în special la nivelul statelor membre. În pofida investițiilor inițiale, crearea routerului central Prüm va reduce costurile pentru statele membre, întrucât prin adoptarea acestei soluții statele membre nu ar mai trebui să creeze (și să mențină) un număr de conexiuni egal cu numărul celorlalte state membre și al categoriilor de date.

- **Drepturile fundamentale**

În conformitate cu Carta drepturilor fundamentale a UE, pe care instituțiile UE și statele membre sunt obligate să o respecte atunci când pun în aplicare dreptul Uniunii [articolul 51 alineatul (1) din cartă], și cu principiul nediscriminării, oportunitățile oferite de opțiunile prezentate trebuie să fie contrabalansate de obligația de a se asigura că eventualele atingeri care ar putea fi aduse drepturilor fundamentale ca urmare a acestor opțiuni sunt limitate la ceea ce este strict necesar pentru a îndeplini în mod efectiv

obiectivele de interes general urmărite, sub rezerva principiului proporționalității [articolul 52 alineatul (1) din cartă].

Soluțiile propuse oferă prilejul adoptării de măsuri preventive specifice de consolidare a securității. Astfel, acestea pot să contribuie la urmărirea obiectivului legitim de facilitare a luptei împotriva criminalității, ceea ce implică și o obligație pozitivă a autorităților de a lua măsuri operative preventive pentru a proteja o persoană a cărei viață este pusă în pericol, în cazul în care au cunoștință sau ar fi trebuit să aibă cunoștință de existența unui risc imediat²⁵.

- **Protecția datelor cu caracter personal**

Schimbul de informații are un impact asupra dreptului la protecția datelor cu caracter personal. Acest drept a fost stabilit prin articolul 8 din cartă, prin articolul 16 din Tratatul privind funcționarea Uniunii Europene și prin articolul 8 din Convenția europeană a drepturilor omului. Așa cum subliniază Curtea de Justiție a UE²⁶, dreptul la protecția datelor cu caracter personal nu este totuși un drept absolut, ci trebuie luat în considerare în raport cu funcția sa în societate. Protecția datelor este strâns legată de respectarea vieții private și a celei de familie, protejată prin articolul 7 din cartă.

În ceea ce privește sistemul Prüm, legislația aplicabilă privind protecția datelor este Directiva (UE) 2016/680. Într-adevăr, cadrul Prüm prevede prelucrarea datelor cu caracter personal efectuată în contextul schimbului de informații între autoritățile de aplicare a legii cu atribuții de prevenire și de cercetare a infracțiunilor.

Libera circulație a datelor în cadrul UE nu trebuie restricționată din motive de protecție a datelor. Trebuie însă îndeplinite o serie de principii. Într-adevăr, pentru a fi legală, orice restrângere a exercițiului drepturilor fundamentale protejate prin cartă trebuie să respecte următoarele criterii, stabilite la articolul 52 alineatul (1):

- (1) să fie prevăzută de lege;
- (2) să respecte substanța drepturilor;
- (3) să răspundă efectiv unor obiective de interes general recunoscute de Uniune sau necesități protejării drepturilor și libertăților celorlalți;
- (4) să fie necesară și
- (5) să fie proporțională.

Prezenta propunere de regulament conține toate aceste norme în materie de protecție a datelor, astfel cum se prevede în detaliu în evaluarea impactului care o însoțește. Propunerea se bazează pe principiile protecției datelor începând cu momentul conceperii și în mod implicit. Aceasta include toate dispozițiile corespunzătoare care limitează prelucrarea datelor la ceea ce este necesar pentru scopul respectiv și care acordă acces la date numai acelor entități care „trebuie să le cunoască”. Accesul la date este rezervat exclusiv personalului autorizat în mod corespunzător care lucrează în cadrul autorităților statelor membre sau al organismelor UE competente pentru scopurile specifice ale cadrului Prüm revizuit și numai în măsura în care aceste date sunt necesare pentru îndeplinirea sarcinilor în conformitate cu aceste scopuri.

²⁵ Curtea Europeană a Drepturilor Omului, Osman/Regatul Unit, nr. 87/1997/871/1083, 28 octombrie 1998, punctul 116.

²⁶ Curtea de Justiție a UE, hotărârea din 9.11.2010 în cauzele conexate C-92/09 și C-93/09 Volker und Markus Schecke și Eifert, Rep., 2010, p. I-0000.

La momentul publicării raportului de evaluare a cursurilor de acțiune pe care statele membre le-au dat [Recomandării Consiliului privind cooperarea polițienească operativă], menționat la punctul 9 litera (d) din recomandarea respectivă, Comisia va decide dacă este necesară o legislație a UE privind cooperarea polițienească operativă transfrontalieră. În cazul în care este nevoie de o astfel de legislație, Comisia va prezenta o propunere legislativă privind cooperarea polițienească operativă transfrontalieră, care va asigura, de asemenea, alinierea dispozițiilor Deciziei 2008/615/JAI și ale Deciziei 2008/616/JAI, care nu au fost reglementate de prezenta propunere, cu Directiva 2016/680, în conformitate cu rezultatele evaluării, în temeiul articolului 62 alineatul (6) din Directiva 2016/680. În cazul în care nu este necesară o legislație a UE privind cooperarea polițienească operativă transfrontalieră, Comisia va prezenta o propunere legislativă pentru a asigura aceeași aliniere, în conformitate cu rezultatele evaluării, în temeiul articolului 62 alineatul (6) din Directiva 2016/680.

4. IMPLICAȚII BUGETARE

Prezenta inițiativă legislativă ar urma să aibă un impact asupra bugetului și a nevoilor de personal ale eu-LISA și ale Europol.

Pentru eu-LISA, se estimează că ar fi nevoie de un buget suplimentar de aproximativ 16 milioane EUR și de aproximativ 10 posturi suplimentare pentru întreaga perioadă a CFM, pentru a se asigura că eu-LISA dispune de resursele necesare pentru a pune în aplicare sarcinile atribuite agenției în prezenta propunere de regulament. Bugetul alocat eu-LISA va fi compensat din IMFV.

Pentru Europol, se estimează că ar fi nevoie de un buget suplimentar de aproximativ 7 milioane EUR și de aproximativ 5 posturi suplimentare pentru întreaga perioadă a CFM, pentru a se asigura că Europol dispune de resursele necesare pentru a-și executa sarcinile atribuite în prezenta propunere de regulament. Bugetul alocat Europol va fi compensat din FSI.

5. ALTE ELEMENTE

- **Planuri de punere în aplicare și măsuri de monitorizare, evaluare și raportare**

Comisia se va asigura că se instituie mecanismele necesare de monitorizare a funcționării măsurilor propuse și le va evalua în raport cu principalele obiective de politică. După doi ani de la instituirea și intrarea în funcțiune a noilor funcționalități și, ulterior, o dată la doi ani, agențiile Uniunii ar trebui să prezinte Parlamentului European, Consiliului și Comisiei un raport privind funcționarea tehnică a noilor măsuri propuse. În plus, la trei ani de la introducerea și utilizarea noilor funcționalități, iar apoi o dată la patru ani, Comisia ar trebui să efectueze o evaluare generală a măsurilor, inclusiv a eventualului impactul direct sau indirect asupra drepturilor fundamentale. Comisia ar trebui să analizeze rezultatele obținute în raport cu obiectivele stabilite, să evalueze dacă principiile de bază sunt în continuare valabile și să identifice eventualele implicații asupra opțiunilor viitoare. Comisia ar trebui să prezinte rapoartele de evaluare Parlamentului European și Consiliului.

- **Explicații detaliate cu privire la dispozițiile specifice ale propunerii**

Capitolul 1 stabilește dispozițiile generale ale prezentului regulament, împreună cu obiectul, scopul și domeniul său de aplicare. Acesta prevede o listă de definiții și reamintește că prelucrarea datelor cu caracter personal în sensul prezentului regulament respectă principiul nediscriminării și alte drepturi fundamentale.

Capitolul 2 stabilește dispozițiile referitoare la schimbul de categorii de date în temeiul prezentului regulament, și anume schimbul de profiluri ADN, date dactiloscopice, date privind înmatricularea vehiculelor, imagini faciale și caziere judiciare. Principiile pentru schimbul de date, căutarea automatizată de date, normele privind solicitările și răspunsurile sunt detaliate într-o secțiune separată

pentru fiecare categorie de date. Capitolul 2 conține, de asemenea, dispoziții comune privind schimbul de date, înființarea de puncte de contact naționale și măsurile de punere în aplicare.

Capitolul 3 stabilește detaliile noii arhitecturi (tehnice) pentru schimbul de date. Prima secțiune a acestui capitol include dispoziții care descriu routerul central, utilizarea routerului și lansarea interogărilor. Vor fi necesare acte de punere în aplicare în care să se specifice procedurile tehnice pentru aceste căutări. Această secțiune include, de asemenea, dispoziții privind interoperabilitatea dintre router și registrul comun de date de identitate cu scopul de a asigura accesul autorităților de aplicare a legii, păstrarea înregistrărilor tuturor operațiunilor de prelucrare a datelor din router, verificarea calității și procedurile de notificare în cazul imposibilității tehnice de a utiliza routerul. O a doua secțiune oferă detalii privind utilizarea Sistemului european de inventariere a cazierelor judiciare (EPRIS) pentru schimbul de caziere judiciare. Această secțiune include, de asemenea, dispoziții privind păstrarea înregistrărilor tuturor operațiunilor de prelucrare de date din EPRIS și procedurile de notificare în cazul imposibilității tehnice de a utiliza EPRIS.

Capitolul 4 stabilește procesele pentru schimbul de date în urma unei concordante. Acesta include o dispoziție privind schimbul automatizat de date de bază, datele fiind limitate la ceea ce este necesar pentru a permite identificarea persoanei în cauză, precum și o dispoziție privind schimbul de date în orice etapă a procesului în temeiul prezentului regulament care nu este descrisă în mod explicit în prezentul regulament.

Capitolul 5 conține dispoziții privind accesul statelor membre la datele biometrice provenite din țări terțe și stocate de Europol și privind accesul Europol la datele stocate în bazele de date ale statelor membre.

Capitolul 6 privind protecția datelor conține dispoziții care asigură faptul că, în temeiul prezentului regulament, datele sunt prelucrate în mod legal și adecvat, în conformitate cu dispozițiile Directivei (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 Consiliului²⁷. Se explică cine va fi persoana împuternicită de operator pentru prelucrarea datelor în temeiul prezentului regulament. În acest capitol se stabilesc măsurile pe care trebuie să le adopte eu-LISA și autoritățile statelor membre pentru a garanta securitatea prelucrării datelor, gestionarea corespunzătoare a incidentelor de securitate și monitorizarea conformității cu măsurile prevăzute în prezentul regulament. Capitolul conține, de asemenea, dispoziții legate de supraveghere și de audit în ceea ce privește protecția datelor. Acesta subliniază principiul conform căruia datele prelucrate în temeiul prezentului regulament nu sunt transferate sau puse la dispoziția niciunei țări terțe sau organizații internaționale în mod automat.

Capitolul 7 detaliază responsabilitățile statelor membre, ale Europol și, respectiv, ale eu-LISA în ceea ce privește punerea în aplicare a măsurilor prevăzute în prezentul regulament.

Capitolul 8 se referă la modificări ale altor acte juridice existente, și anume ale Deciziilor 2008/615/JAI și 2008/616/JAI, ale Regulamentului (UE) 2018/1726, ale Regulamentului (UE) 2019/817 și ale Regulamentului (UE) 2019/818.

Capitolul 9, care cuprinde dispozițiile finale, stabilește detaliile referitoare la raportare și statistici, costuri, notificări, dispozițiile tranzitorii și derogări. Acesta stabilește, de asemenea, cerințele pentru

²⁷ În conformitate cu concluziile Comisiei enunțate în Comunicarea sa din 24 iunie 2020 „Calea de urmat pentru alinierea acquis-ului din fostul al treilea pilon la normele privind protecția datelor [COM(2020) 262 final].

începerea punerii în aplicare a măsurilor propuse în temeiul prezentului regulament. Capitolul prevede și instituirea unui comitet și adoptarea unui manual practic pentru a sprijini punerea în aplicare și gestionarea prezentului regulament. Sunt incluse, de asemenea, o dispoziție privind monitorizarea și evaluarea și o dispoziție privind intrarea în vigoare și aplicabilitatea prezentului regulament. În special, prezentul regulament înlocuiește articolele 2-6 și secțiunile 2 și 3 ale capitolului 2 din Decizia 2008/615/JAI a Consiliului, precum și capitolele 2-5 și articolele 18, 20 și 21 din Decizia 2008/616/JAI a Consiliului, care, în consecință, vor fi eliminate din respectivele decizii ale Consiliului de la data aplicării prezentului regulament. Efectul acestor modificări va fi acela că dispozițiile înlocuite și eliminate nu se vor mai aplica niciunui stat membru.

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind schimbul automatizat de date în scopul cooperării polițienești („Prüm II”), de modificare a Deciziilor 2008/615/JAI și 2008/616/JAI ale Consiliului și a Regulamentelor (UE) 2018/1726, 2019/817 și 2019/818 ale Parlamentului European și ale Consiliului

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 European²⁸,

având în vedere avizul Comitetului Regiunilor²⁹,

hotărând în conformitate cu procedura legislativă ordinară,

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 ar trebui să se realizeze, printre altele, prin intermediul unor măsuri adecvate de prevenire și combatere a criminalității, inclusiv a criminalității organizate și a terorismului.
- (2) Acest obiectiv impune ca autoritățile de aplicare a legii să facă schimb de date, în mod eficient și în timp util, pentru a combate în mod eficace criminalitatea.
- (3) Prin urmare, obiectivul prezentului regulament este de a îmbunătăți, eficientiza și facilita schimbul de informații în materie penală între autoritățile de aplicare a legii din statele membre, dar și cu Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii, instituită prin Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului³⁰ (Europol) ca centru de informații în materie penală al Uniunii.
- (4) Deciziile 2008/615/JAI³¹ și 2008/616/JAI³² ale Consiliului de stabilire a normelor pentru schimbul de informații între autoritățile cu atribuții de prevenire și cercetare a infracțiunilor prin

²⁸JO C , , p. .

²⁹JO C , , p. .

³⁰ 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).

³¹ 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).

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.

- (5) Prezentul regulament ar trebui să stabilească condițiile și procedurile pentru transferul automatizat de profiluri ADN, date dactiloscopice, date privind înmatricularea vehiculelor, imagini faciale și caziere judiciare. Acest lucru nu ar trebui să aducă atingere prelucrării oricăreia dintre aceste date în Sistemul de Informații Schengen (SIS), schimbului de informații suplimentare referitoare la acestea prin intermediul birourilor SIRENE sau drepturilor persoanelor ale căror date sunt prelucrate în cadrul acestora.
- (6) Prelucrarea datelor cu caracter personal și schimbul de date cu caracter personal în sensul prezentului regulament nu ar trebui să conducă la discriminarea persoanelor din niciun motiv. Acestea 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) Prin asigurarea căutării sau a comparării automatizate a profilurilor ADN, a datelor dactiloscopice, a datelor privind înmatricularea vehiculelor, a imaginilor faciale și a cazierelor judiciare, scopul prezentului regulament este, de asemenea, de a facilita căutarea persoanelor dispărute și a rămășițelor umane neidentificate. Acest lucru nu ar trebui să aducă atingere introducerii semnalărilor SIS cu privire la persoane dispărute și schimbului de informații suplimentare cu privire la aceste semnalări în temeiul Regulamentului (UE) 2018/1862 al Parlamentului European și al Consiliului³².
- (8) Directiva (UE) .../... [privind *schimbul de informații între autoritățile de aplicare a legii din statele membre*] oferă un cadru juridic coerent al Uniunii pentru a se asigura că autoritățile de aplicare a legii au acces echivalent la informațiile deținute de alte state membre atunci când au nevoie de acestea pentru a combate criminalitatea și terorismul. Pentru a consolida schimbul de informații, directiva formalizează și clarifică procedurile pentru schimburile de informații între statele membre, în special în scopul desfășurării anchetelor, inclusiv rolul „punctului unic de contact” pentru astfel de schimburi, precum și utilizarea deplină a canalului de schimb de informații SIENA. Orice schimb de informații în afara celor prevăzute în prezentul regulament ar trebui reglementat prin Directiva (UE) .../... [privind *schimbul de informații între autoritățile de aplicare a legii din statele membre*].
- (9) Pentru căutarea automatizată a datelor privind înmatricularea vehiculelor, statele membre 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), conceput în acest scop. EUCARIS ar trebui să conecteze 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.

³² 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).

³³ 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).

- (10) Identificarea unui infractor este esențială pentru succesul cercetării și urmăririi penale. Căutarea automatizată a imaginilor faciale ale suspecților și infractorilor condamnați ar trebui să ofere informații suplimentare pentru identificarea cu succes a infractorilor și pentru combaterea criminalității.
- (11) Căutarea sau compararea automatizată a datelor biometrice (profiluri ADN, date dactiloscopice și imagini faciale) între autoritățile responsabile cu prevenirea, depistarea și cercetarea infracțiunilor în temeiul prezentului regulament ar trebui să vizeze numai datele conținute în bazele de date create pentru prevenirea, depistarea și cercetarea infracțiunilor.
- (12) Participarea la schimbul de cazieri judiciare ar trebui să rămână voluntară. În cazul în care statele membre decid să participe, în spiritul reciprocității, acestea nu ar trebui să aibă posibilitatea de a efectua interogări în bazele de date ale altor state membre dacă nu pun la dispoziție propriile date pentru interogări efectuate de celelalte state membre.
- (13) În ultimii ani, Europol a primit un volum mare de date biometrice ale teroriștilor și infractorilor suspecți și condamnați din mai multe țări terțe. Includerea datelor provenite din țări terțe și stocate la nivelul Europol în cadrul Prüm și, prin urmare, punerea acestor date la dispoziția autorităților de aplicare a legii sunt necesare pentru o mai bună prevenire și cercetare a infracțiunilor. Acestea contribuie, de asemenea, la crearea de sinergii între diferitele instrumente de asigurare a respectării legii.
- (14) În temeiul cadrului Prüm, Europol ar trebui să poată efectua căutări în bazele de date ale statelor membre cu date primite de la țări terțe, pentru a stabili legături transfrontaliere între cauzele penale. Posibilitatea de a utiliza datele Prüm, alături de alte baze de date aflate la dispoziția Europol, ar trebui să faciliteze efectuarea unei analize mai complete și mai documentate cu privire la cercetările penale și ar trebui să permită Europol să sprijine mai bine autoritățile de aplicare a legii din statele membre. În cazul unei concordanțe între datele utilizate pentru căutare și datele deținute în bazele de date ale statelor membre, statele membre pot furniza Europol informațiile necesare pentru îndeplinirea atribuțiilor sale.
- (15) 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 acestei arhitecturi tehnice, fiecare stat membru ar trebui să stabilească cel puțin 26 de conexiuni, ceea ce înseamnă o conexiune cu fiecare stat membru pentru fiecare categorie de date. Routerul și Sistemul european de inventariere a cazierelor judiciare (EPRIS) instituit prin prezentul regulament ar trebui să simplifice arhitectura tehnică a cadrului Prüm și să servească 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 în ceea ce privește cazierele judiciare.
- (16) Routerul ar trebui să fie conectat la portalul european de căutare instituit prin articolul 6 din Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului³⁴ și prin articolul 6 din Regulamentul (UE) 2019/818 al Parlamentului European și al Consiliului³⁵, pentru a

³⁴ 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).

³⁵ 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

permite autorităților statelor membre și Europol să lanseze interogări în bazele de date naționale în temeiul prezentului regulament simultan cu interogările în registrul comun de date de identitate instituit prin articolul 17 din Regulamentul (UE) 2019/817 și prin articolul 17 din Regulamentul (UE) 2019/818 în scopul asigurării respectării legii.

- (17) În cazul unei concordanțe între datele utilizate pentru căutare sau comparare și datele deținute în baza de date națională a statului membru (statelor membre) solicitat(e) și după confirmarea acestei concordanțe de către statul membru solicitant, statul membru solicitat ar trebui să returneze prin router un set limitat de date de bază în termen de 24 de ore. Acest termen ar urma să asigure un schimb rapid de informații între autoritățile statelor membre. Statele membre ar trebui să păstreze controlul asupra transmiterii acestui set limitat de date de bază. Un anumit grad de intervenție umană ar trebui menținut în momentele-cheie ale procesului, inclusiv în ceea ce privește decizia de a transmite date cu caracter personal statului membru solicitant, pentru a se asigura că nu va exista niciun schimb automatizat de date de bază.
- (18) Orice schimb de informații între autoritățile statelor membre sau cu Europol în orice etapă a unui dintre procesele descrise în prezentul regulament, care nu este descris în mod explicit în prezentul regulament, ar trebui să aibă loc prin intermediul SIENA, pentru a se asigura că toate statele membre utilizează un canal comun, securizat și fiabil de comunicare.
- (19) La dezvoltarea routerului și a sistemului EPRIS ar trebui utilizat standardul privind formatul universal pentru mesaje (*universal message format* - UMF). Orice schimb automatizat de date în conformitate cu prezentul regulament ar trebui să utilizeze standardul UMF. Autoritățile statelor membre și Europol sunt încurajate să utilizeze standardul UMF și în legătură cu orice alt schimb de date între acestea în contextul cadrului Prüm II. 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.
- (20) Doar informațiile neclasificate ar trebui să facă obiectul schimburilor prin intermediul cadrului Prüm II.
- (21) 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 și elementele de date care urmează să facă obiectul schimbului. În vederea asigurării unor condiții uniforme de punere în aplicare a prezentului regulament, Comisia ar trebui investită cu competențe de executare. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului³⁶.
- (22) Întrucât prezentul regulament prevede instituirea noului cadru Prüm, dispozițiile relevante ale Deciziilor 2008/615/JAI și 2008/616/JAI ar trebui eliminate. Prin urmare, ar trebui ca deciziile respective să fie modificate în consecință.
- (23) Întrucât routerul ar trebui dezvoltat și gestionat de Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție, instituită prin Regulamentul (UE) 2018/1726 al Parlamentului European și

azilului și al migrației și de modificare a Regulamentelor (UE) 2018/1726, 2018/1862 și 2019/816 (JO L 135, 22.5.2019, p. 85).

³⁶ 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).

al Consiliului³⁷ (eu-LISA), este necesar, prin urmare, să se modifice Regulamentul (UE) 2018/1726 prin adăugarea acestei atribuții a agenției. Prin urmare, pentru ca routerul să poată fi conectat la portalul european de căutare și să efectueze căutări simultane în router și în registrul comun de date de identitate, este necesar să se modifice Regulamentul (UE) 2019/817. Pentru ca routerul să poată fi conectat la portalul european de căutare în vederea efectuării de căutări simultane în router și în registrul comun de date de identitate și a stocării rapoartelor și statisticilor routerului în registrul comun de raportare și statistici, este necesar, prin urmare, să se modifice Regulamentul (UE) 2019/818. Așadar, este necesar ca regulamentele respective să fie modificate în consecință.

- (24) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu participă la adoptarea prezentului regulament, nu are obligații în temeiul acestuia și nu face obiectul aplicării sale.
- (25) [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 Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Irlanda și-a notificat intenția de a participa la adoptarea și la aplicarea prezentului regulament.] SAU [În conformitate cu articolele 1 și 2 din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene și, fără a aduce atingere articolului 4 din protocolul menționat, Irlanda nu participă la adoptarea prezentului regulament, nu are obligații în temeiul acestuia și nu face obiectul aplicării sale.]
- (26) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului³⁸ și a emis un aviz la [XX]³⁹.

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL 1

DISPOZIȚII GENERALE

Articolul 1

Obiectul

Prezentul regulament stabilește un cadru pentru schimbul de informații între autoritățile responsabile cu prevenirea, depistarea și cercetarea infracțiunilor (Prüm II).

³⁷ 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 Lărgă 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).

³⁸ 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).

³⁹ [JO C ...].

Prezentul regulament prevede condițiile și procedurile pentru căutarea automatizată de profiluri ADN, de date dactiloscopice, de imagini faciale, de caziere judiciare și de anumite date privind înmatricularea vehiculelor, precum și normele privind schimbul de date de bază în urma unei concordanțe.

Articolul 2

Scopul

Scopul Prüm II este de a intensifica cooperarea transfrontalieră în domeniile reglementate de partea III titlul V capitolul 5 din Tratatul privind funcționarea Uniunii Europene, în special schimbul de informații între autoritățile responsabile cu prevenirea, depistarea și cercetarea infracțiunilor.

De asemenea, Prüm II are scopul de a le permite autorităților responsabile cu prevenirea, depistarea și cercetarea infracțiunilor să efectueze căutări ale persoanelor dispărute și ale rămășițelor umane neidentificate.

Articolul 3

Domeniul de aplicare

Prezentul regulament se aplică bazelor de date naționale utilizate pentru transferul automatizat al următoarelor categorii de date: profiluri ADN, date dactiloscopice, imagini faciale, caziere judiciare și anumite date privind înmatricularea vehiculelor.

Articolul 4

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

- (1) „loci” înseamnă structura moleculară specifică din diferitele segmente de ADN;
- (2) „profil ADN” înseamnă un cod alfabetic sau numeric care reprezintă un set de caracteristici de identificare a părții necodate a unui eșantion analizat de ADN uman, și anume structura moleculară specifică din diverse segmente de ADN;
- (3) „partea necodificată a ADN-ului” înseamnă zone de cromozomi care nu conțin nicio expresie genetică, și anume despre care nu se știe că ar furniza informații referitoare la proprietățile funcționale ale unui organism;
- (4) „date de referință ADN” înseamnă un profil ADN și numărul de referință menționat la articolul 9;
- (5) „profil ADN de referință” înseamnă profilul ADN al unei persoane identificate;
- (6) „profil ADN neidentificat” înseamnă profilul ADN obținut din indiciile culese în timpul cercetării unor infracțiuni și care aparține unei persoane neidentificate încă;
- (7) „date dactiloscopice” înseamnă imagini de amprente digitale, imagini de amprente digitale latente, amprente palmare, amprente palmare latente, precum și șabloane ale unor astfel de imagini (caracteristici codificate ale acestora) atunci când sunt stocate și prelucrate într-o bază de date automatizată;
- (8) „date dactiloscopice de referință” înseamnă date dactiloscopice și numărul de referință menționat la articolul 14;
- (9) „caz individual” înseamnă un singur dosar de anchetă;

- (10) „imagine facială” înseamnă imaginea digitală a feței;
- (11) „date biometrice” înseamnă profiluri ADN, date dactiloscopice sau imagini faciale;
- (12) „concordanță” înseamnă existența unei corespondențe care reiese din compararea automatizată a unor date cu caracter personal care sunt înregistrate sau sunt în curs de a fi înregistrate într-un sistem de informații sau într-o bază de date;
- (13) „candidat” înseamnă datele pentru care s-a obținut o concordanță;
- (14) „stat membru solicitant” înseamnă statul membru care efectuează o căutare prin intermediul sistemului Prüm II;
- (15) „stat membru solicitat” înseamnă statul membru în ale cărui baze de date statul membru solicitant efectuează căutarea prin intermediul sistemului Prüm II;
- (16) „cazier judiciar” înseamnă orice informație disponibilă în registrul național sau în registrele naționale în care sunt înregistrate date ale autorităților competente în scopul prevenirii, depistării și cercetării infracțiunilor;
- (17) „pseudonimizare” înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anumite persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie păstrate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică prin care să se asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;
- (18) „date Europol” înseamnă orice date cu caracter personal prelucrate de Europol în conformitate cu Regulamentul (UE) 2016/794;
- (19) „autoritate de supraveghere” înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 41 din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului⁴⁰;
- (20) „SIENA” înseamnă aplicația de rețea securizată pentru schimbul de informații, gestionată de Europol, menită să faciliteze schimbul de informații între statele membre și Europol;
- (21) „incident semnificativ” înseamnă orice incident, cu excepția cazului în care are un impact redus și este probabil să fie deja bine înțeles în ceea ce privește metoda sau tehnologia;
- (22) „amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică cu intenția, ocazia și capacitatea de a provoca un incident semnificativ;
- (23) „vulnerabilitate semnificativă” înseamnă o vulnerabilitate care poate duce la un incident semnificativ dacă este exploatată;
- (24) „incident” înseamnă un incident în sensul articolului 4 alineatul (5) din Directiva (UE) .../... a Parlamentului European și a Consiliului⁴¹ [*propunerea de Directivă privind NIS 2*].

⁴⁰ 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).

⁴¹ Directiva (UE) .../... a Parlamentului European și a Consiliului ... (JO ...).

CAPITOLUL 2

SCHIMBUL DE DATE

SECȚIUNEA 1

Profiluri ADN

Articolul 5

Crearea fișierelor naționale de analiză ADN

(1) Statele membre deschid și mențin fișiere naționale de analiză ADN în vederea cercetării infracțiunilor.

În temeiul prezentului regulament, prelucrarea datelor înregistrate în aceste fișiere se efectuează în conformitate cu prezentul regulament, cu respectarea legislației naționale a statelor membre care este aplicabilă procedurii de prelucrare a datelor respective.

(2) Statele membre asigură disponibilitatea datelor de referință ADN din fișierele lor naționale de analiză ADN menționate la alineatul (1).

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

Datele de referință ADN care nu sunt atribuite niciunei persoane („profiluri ADN neidentificate”) trebuie să poată fi recunoscute ca atare.

Articolul 6

Căutarea automatizată a profilurilor ADN

(1) Statele membre permit punctelor de contact naționale menționate la articolul 29 și Europolului accesul la datele de referință ADN din fișierele lor de analiză ADN, pentru a efectua căutări automatizate prin compararea profilurilor ADN în scopul cercetării infracțiunilor.

Căutările pot fi efectuate numai în cazuri individuale și în conformitate cu dreptul intern al statului membru solicitant.

(2) În cazul în care o căutare automatizată indică o concordanță între un profil ADN furnizat și un profil ADN înregistrat în fișierul analizat al statului membru solicitat, 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.

În cazul în care nu există nicio concordanță, statului membru solicitant i se transmite o notificare automatizată în acest sens.

(3) Punctul de contact național al statului membru solicitant confirmă o concordanță între datele privind profilurile ADN și datele de referință ADN deținute de statul membru solicitat în urma furnizării automatizate a datelor de referință ADN necesare pentru confirmarea unei concordanțe.

Articolul 7

Compararea automatizată a profilurilor ADN neidentificate

(1) În vederea cercetării infracțiunilor, statele membre pot compara, prin intermediul punctelor lor de contact naționale, profilurile ADN neidentificate pe care le dețin cu toate profilurile ADN din alte

fișiere naționale de analiză ADN. Furnizarea și compararea profilurilor se realizează în mod automatizat.

(2) În cazul în care, ca urmare a comparării menționate la alineatul (1), un stat membru solicitat constată că există o concordanță între un profil ADN furnizat și un profil din propriile sale fișiere de analiză ADN, acesta comunică fără întârziere punctului de contact național al statului membru solicitant datele de referință ADN în raport cu care a fost constatată concordanța.

(3) Confirmarea unei concordanțe între profilurile ADN și datele de referință ADN deținute de statul membru solicitat se realizează de punctul de contact național al statului membru solicitant în urma furnizării automatizate a datelor de referință ADN necesare pentru confirmare unei concordanțe.

Articolul 8

Raportarea cu privire la fișierele de analiză ADN

Fiecare stat membru informează Comisia și eu-LISA cu privire la fișierele naționale de analiză ADN cărora li se aplică articolele 5-7, în conformitate cu articolul 73.

Articolul 9

Numerele de referință pentru profilurile ADN

Numerele de referință pentru profilurile ADN reprezintă combinația dintre:

- (a) un număr de referință prin intermediul căruia statele membre, în cazul unei concordanțe, pot extrage date suplimentare și alte informații din bazele lor de date menționate la articolul 5 pentru a le furniza unuia, mai multor sau tuturor celorlalte state membre, în conformitate cu articolele 47 și 48;
- (b) un cod care indică statul membru care deține profilul ADN;
- (c) un cod care indică tipul de profil ADN (profil ADN de referință sau profil ADN neidentificat).

Articolul 10

Principiile schimbului de date de referință ADN

(1) Se adoptă măsuri corespunzătoare pentru a se asigura confidențialitatea și integritatea datelor de referință ADN trimise către alte state membre, inclusiv criptarea acestora.

(2) Statele membre iau măsurile necesare pentru a garanta integritatea profilurilor ADN puse la dispoziția celorlalte state membre sau trimise acestora spre comparare și pentru a se asigura că aceste măsuri respectă standardele internaționale relevante pentru schimbul de date de referință ADN.

(3) Comisia adoptă acte de punere în aplicare pentru a specifica standardele internaționale relevante care trebuie să fie utilizate de statele membre pentru schimbul de date de referință ADN. Respectivetele acte de punere în aplicare se adoptă în conformitate cu procedura menționată la articolul 76 alineatul (2).

Articolul 11

Norme privind solicitările și răspunsurile referitoare la profilurile ADN

(1) O solicitare de căutare sau comparare automatizată include numai informațiile următoare:

- (a) codul statului membru solicitant;

- (b) data, ora și numărul de referință al solicitării;
 - (c) profilurile ADN și numerele de referință ale acestora menționate la articolul 9;
 - (d) tipurile de profiluri ADN transmise (profiluri ADN neidentificate sau profiluri ADN de referință).
- (2) Răspunsul la solicitarea menționată la alineatul (1) conține numai informațiile următoare:
- (a) o precizare dacă a existat una sau au existat mai multe concordanțe sau dacă nu a existat nicio concordanță;
 - (b) data, ora și numărul de referință al solicitării;
 - (c) data, ora și numărul de referință al 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) tipul profilurilor ADN transmise (profiluri ADN neidentificate sau profiluri ADN de referință);
 - (g) profilurile ADN între care s-a stabilit o concordanță.
- (3) Notificarea automatizată a unei concordanțe este furnizată numai dacă în urma căutării sau a comparării automatizate a rezultat o concordanță cu un număr minim de loci. Comisia adoptă acte de punere în aplicare pentru a specifica acest număr minim de loci, în conformitate cu procedura menționată la articolul 76 alineatul (2).
- (4) În cazul în care o căutare sau o comparare cu profiluri ADN neidentificate conduce la o concordanță, fiecare stat membru solicitat care deține date între care s-a stabilit o concordanță 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 sau a comparării efectuate de un alt stat membru.
- (5) Statele membre se asigură că solicitările sunt coerente cu declarațiile transmise în temeiul articolului 8. Declarațiile respective sunt reproduse în manualul practic menționat la articolul 78.

SECȚIUNEA 2

Date dactiloscopice

Articolul 12

Date dactiloscopice de referință

- (1) Statele membre asigură disponibilitatea datelor dactiloscopice de referință din dosar pentru sistemele naționale automatizate de identificare a amprentelor digitale instituite în scopul prevenirii, depistării și cercetării infracțiunilor.
- (2) Datele dactiloscopice de referință nu conțin niciun fel de date care să permită identificarea directă a unei persoane.
- (3) Datele dactiloscopice de referință care nu sunt atribuite niciunei persoane fizice (date dactiloscopice neidentificate) trebuie să poată fi recunoscute ca atare.

Articolul 13

Căutarea automatizată a datelor dactiloscopice

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

Căutările pot fi efectuate numai în cazuri individuale și în conformitate cu dreptul intern al statului membru solicitant.

(2) Punctul de contact național al statului membru solicitant confirmă o concordanță a datelor dactiloscopice cu datele dactiloscopice de referință deținute de statul membru solicitat în urma transmiterii automatizate a datelor dactiloscopice necesare pentru confirmarea unei concordanțe.

Articolul 14

Numerele de referință pentru datele dactiloscopice

Numerele de referință pentru datele dactiloscopice reprezintă combinația dintre:

- (a) un număr de referință prin intermediul căruia statele membre, în cazul unei concordanțe, pot extrage date suplimentare și alte informații din bazele lor de date menționate la articolul 12 pentru a le furniza unuia, mai multor sau tuturor celorlalte state membre, în conformitate cu articolele 47 și 48;
- (b) un cod care indică statul membru care deține datele dactiloscopice.

Articolul 15

Principii pentru schimbul de date dactiloscopice

(1) Digitalizarea datelor dactiloscopice și transmiterea acestora către celelalte state membre se efectuează în conformitate cu un format uniform de date. Comisia adoptă acte de punere în aplicare pentru a specifica formatul uniform de date în conformitate cu procedura menționată la articolul 76 alineatul (2).

(2) Fiecare stat membru se asigură că datele dactiloscopice pe care le transmite sunt de o calitate suficientă pentru a permite compararea acestora cu ajutorul sistemelor automatizate de identificare a amprentelor digitale.

(3) Statele membre adoptă măsuri corespunzătoare pentru a asigura confidențialitatea și integritatea datelor dactiloscopice trimise altor state membre, inclusiv criptarea acestora.

(4) Comisia adoptă acte de punere în aplicare pentru a specifica standardele relevante existente pentru schimbul de date dactiloscopice care trebuie să fie utilizate de statele membre. Respectivile acte de punere în aplicare se adoptă în conformitate cu procedura menționată la articolul 76 alineatul (2).

Articolul 16

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.

Statele membre informează Comisia și eu-LISA, în conformitate cu articolul 79 alineatele (8) și (10), cu privire la capacitățile lor maxime de căutare pe zi pentru datele dactiloscopice ale persoanelor identificate și pentru datele dactiloscopice ale persoanelor care nu au fost încă identificate.

(2) Comisia adoptă acte de punere în aplicare pentru a specifica numărul maxim de candidați acceptați pentru comparație pentru fiecare transmitere în conformitate cu procedura menționată la articolul 76 alineatul (2).

Articolul 17

Norme privind solicitările și răspunsurile referitoare la datele dactiloscopice

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

- (a) codul statului membru solicitant;
- (b) data, ora și numărul de referință al solicitării;
- (c) datele dactiloscopice și numerele de referință ale acestora menționate la articolul 14.

(2) Răspunsul la solicitarea 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, ora și numărul de referință al solicitării;
- (c) data, ora și numărul de referință al 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.

SECȚIUNEA 3

Date privind înmatricularea vehiculelor

Articolul 18

Căutarea automatizată a datelor privind înmatricularea vehiculelor

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

- (a) datele referitoare la proprietari sau la utilizatori;
- (b) datele referitoare la vehicule.

(2) Căutările pot fi efectuate doar prin utilizarea unui număr complet de șasiu sau a unui număr complet de înmatriculare.

(3) Căutările pot fi efectuate numai în conformitate cu legislația națională a statului membru solicitant.

Articolul 19

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 sistemul Eucaris se transmit într-o formă criptată.
- (3) Comisia adoptă acte de punere în aplicare pentru a specifica elementele datelor privind înmatricularea vehiculelor care trebuie să facă obiectul schimburilor. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura menționată la articolul 76 alineatul (2).

Articolul 20

Păstrarea înregistrărilor

- (1) Fiecare stat membru păstrează înregistrări ale interogărilor efectuate de personalul autorităților sale 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) statul membru sau agenția Uniunii care a lansat solicitarea de interogare;
 - (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) pot fi 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.
Acele înregistrări se protejează prin măsuri corespunzătoare împotriva accesului neautorizat și se șterg după o perioadă de un an 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 este nevoie de ele 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 56.

SECȚIUNEA 4

Imagini faciale

Articolul 21

Imagini faciale

- (1) Statele membre asigură disponibilitatea imaginilor faciale din bazele lor de date naționale instituite în scopul prevenirii, depistării și cercetării infracțiunilor. Aceste date includ numai imagini faciale și

numărul de referință menționat la articolul 23 și indică dacă imaginile faciale sunt atribuite unei persoane sau nu.

Statele membre nu pun la dispoziție în acest context date care să permită identificarea directă a unei persoane.

(2) Imaginile faciale care nu sunt atribuite niciunei persoane (imagini faciale neidentificate) trebuie să poată fi recunoscute ca atare.

Articolul 22

Căutarea automatizată a imaginilor faciale

(1) În scopul prevenirii, depistării și cercetării infracțiunilor, statele membre permit punctelor de contact naționale ale altor state membre și Europolului accesul la imaginile faciale stocate în bazele lor de date naționale, pentru a efectua căutări automatizate.

Căutările pot fi efectuate numai în cazuri individuale și în conformitate cu dreptul intern al statului membru solicitant.

(2) Statul membru solicitant primește o listă alcătuită din concordanțe privind candidații potențiali. Statul membru respectiv analizează lista pentru a stabili existența unei concordanțe confirmate.

(3) Se stabilește un standard minim de calitate pentru a permite căutarea și compararea imaginilor faciale. Comisia adoptă acte de punere în aplicare pentru a specifica standardul minim de calitate. Respectivetele acte de punere în aplicare se adoptă în conformitate cu procedura menționată la articolul 76 alineatul (2).

Articolul 23

Numerele de referință pentru imaginile faciale

Numerele de referință pentru imaginile faciale reprezintă combinația dintre:

- (a) un număr de referință prin intermediul căruia statele membre, în cazul unei concordanțe, pot extrage date suplimentare și alte informații din bazele lor de date menționate la articolul 21 pentru a le furniza unuia, mai multor sau tuturor celorlalte state membre, în conformitate cu articolele 47 și 48;
- (b) un cod care indică statul membru care deține imaginile faciale.

Articolul 24

Norme privind solicitările și răspunsurile referitoare la imaginile faciale

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

- (a) codul statului membru solicitant;
- (b) data, ora și numărul de referință al solicitării;
- (c) imaginile faciale și numerele de referință ale acestora menționate la articolul 23.

(2) Răspunsul la solicitarea 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, ora și numărul de referință al solicitării;

- (c) data, ora și numărul de referință al 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.

SECȚIUNEA 5

Caziere judiciare

Articolul 25

Caziere judiciare

(1) Statele membre pot decide să participe la schimbul automatizat de caziere judiciare. Statele membre care participă la schimbul automatizat de caziere judiciare asigură disponibilitatea datelor biografice ale suspectilor și infractorilor din registrele naționale ale cazierelor judiciare întocmite pentru cercetarea infracțiunilor. Acest set de date, dacă este disponibil, conține următoarele date:

- (a) prenumele;
- (b) numele;
- (c) pseudonimul (pseudonimele);
- (d) data nașterii;
- (e) cetățenia sau cetățeniile;
- (f) locul și țara nașterii;
- (g) genul.

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

Articolul 26

Căutarea automatizată a cazierelor judiciare

(1) În scopul cercetării infracțiunilor, statele membre permit punctelor de contact naționale ale altor state membre și Europolului accesul la datele din registrele naționale ale cazierelor judiciare, pentru a efectua căutări automatizate.

Căutările pot fi efectuate numai în cazuri individuale și în conformitate cu dreptul intern al statului membru solicitant.

(2) Statul membru solicitant primește lista de concordanțe cu o indicare a calității concordanțelor.

Statul membru solicitant trebuie să fie informat și cu privire la statul membru a cărui bază de date conține date care au condus la o concordanță.

Articolul 27

Numerele de referință pentru cazierele judiciare

Numerele de referință pentru cazierele judiciare reprezintă combinația dintre:

- (a) un număr de referință prin intermediul căruia statele membre, în cazul unei concordanțe, pot extrage date cu caracter personal și alte informații din registrele menționate la articolul 25 pentru a le furniza unuia, mai multor sau tuturor celorlalte state membre, în conformitate cu articolele 47 și 48;
- (b) un cod care indică statul membru care deține cazierul judiciar.

Articolul 28

Norme privind solicitările și răspunsurile referitoare la cazierul judiciar

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

- (a) codul statului membru solicitant;
- (b) data, ora și numărul de referință al solicitării;
- (c) cazierul judiciar și numerele de referință ale acestora menționate la articolul 27.

(2) Răspunsul la solicitarea 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, ora și numărul de referință al solicitării;
- (c) data, ora și numărul de referință al răspunsului;
- (d) codul statului membru solicitant și cel al statului membru solicitat;
- (e) numerele de referință ale cazierelor judiciare din statele membre solicitate.

SECȚIUNEA 6

Dispoziții comune

Articolul 29

Puncte de contact naționale

Fiecare stat membru desemnează un punct de contact național.

Punctele de contact naționale au responsabilitatea de a furniza datele menționate la articolele 6, 7, 13, 18, 22 și 26.

Articolul 30

Măsuri de punere în aplicare

Comisia adoptă acte de punere în aplicare pentru a specifica modalitățile tehnice ale procedurilor prevăzute la articolele 6, 7, 13, 18, 22 și 26. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura menționată la articolul 76 alineatul (2).

Articolul 31

Specificații tehnice

Statele membre și Europol respectă specificațiile tehnice comune în legătură cu toate solicitările și răspunsurile referitoare la căutările și comparările de profiluri ADN, date dactiloscopice, date privind

înmatricularea vehiculelor, imagini faciale și caziere judiciare. Comisia adoptă acte de punere în aplicare pentru a preciza aceste specificații tehnice în conformitate cu procedura menționată la articolul 76 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 sau comparări automatizate de date ADN, date dactiloscopice și date privind înmatricularea vehiculelor 24 de ore pe zi, 7 zile pe săptămână.

(2) Punctele de contact naționale se informează reciproc și informează Comisia, Europol și eu-LISA, fără întârziere, cu privire la orice defecțiune tehnică care cauzează indisponibilitatea schimbului automatizat de date.

Punctele de contact naționale convin asupra unor modalități alternative temporare pentru schimbul de informații în conformitate cu dreptul aplicabil al Uniunii și cu legislația națională aplicabilă.

(3) Punctele de contact naționale restabilesc fără întârziere schimbul automatizat de date.

Articolul 33

Justificarea prelucrării datelor

(1) Fiecare stat membru păstrează justificarea interogărilor pe care le efectuează autoritățile sale competente.

Europol păstrează justificarea interogărilor pe care le efectuează.

(2) Justificarea menționată la alineatul (1) cuprinde:

- (a) scopul interogării, inclusiv o referire la cazul sau cercetarea respectivă;
- (b) o precizare dacă interogarea se referă la un suspect sau la un autor al unei infracțiuni;
- (c) o precizare dacă interogarea vizează identificarea unei persoane necunoscute sau obținerea mai multor date cu privire la o persoană cunoscută.

(3) Justificările menționate la alineatul (2) trebuie să fie folosite numai pentru monitorizarea protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, precum și pentru asigurarea securității și integrității datelor.

Aceste justificări se protejează prin măsuri corespunzătoare împotriva accesului neautorizat și se șterg după o perioadă de un an 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 este nevoie de aceste justificări 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 aceste justificări pentru automonitorizarea menționată la articolul 56.

Articolul 34

Utilizarea formatului universal pentru mesaje

- (1) La dezvoltarea routerului menționat la articolul 35 și a sistemului EPRIS se utilizează standardul privind formatul universal pentru mesaje (UMF).
- (2) Orice schimb automatizat de date în conformitate cu prezentul regulament utilizează standardul UMF.

CAPITOLUL 3

ARHITECTURA

SECȚIUNEA 1

Routerul

Articolul 35

Routerul

- (1) Se instituie un router cu scopul de a facilita stabilirea de conexiuni între statele membre și cu Europol pentru interogarea, extragerea și evaluarea datelor biometrice 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 ale statelor membre menționate la articolele 5, 12 și 21, precum și a datelor Europol;
 - (b) un canal securizat de comunicații între infrastructura centrală, statele membre și agențiile Uniunii care au dreptul să utilizeze routerul;
 - (c) o infrastructură de comunicații securizată între infrastructura centrală și portalul european de căutare în sensul articolului 39.

Articolul 36

Utilizarea routerului

Utilizarea routerului este rezervată pentru autoritățile statelor membre care au acces la schimbul de profiluri ADN, de date dactiloscopice și de imagini faciale, precum și pentru Europol, în conformitate cu prezentul regulament și cu Regulamentul (UE) 2016/794.

Articolul 37

Interogările

- (1) Utilizatorii routerului menționați la articolul 36 solicită o interogare prin transmiterea de date biometrice către router. Routerul trimite solicitarea de interogare către bazele de date ale statelor membre și către datele Europol simultan cu datele transmise de utilizator și în conformitate cu drepturile de acces ale acestora.
- (2) La primirea solicitării de interogare din partea routerului, fiecare stat membru solicitat și Europol lansează o interogare în bazele lor de date în mod automatizat și fără întârziere.

- (3) Toate concordanțele rezultate în urma interogării în bazele de date ale fiecărui stat membru și în datele Europol sunt trimise înapoi în mod automatizat routerului.
- (4) Routerul clasifică răspunsurile în funcție de scorul corespondenței dintre datele biometrice utilizate pentru interogare și datele biometrice stocate în bazele de date ale statelor membre și în datele Europol.
- (5) Lista datelor biometrice între care s-a stabilit o concordanță și punctajele acestora sunt returnate utilizatorului routerului de către router.
- (6) Comisia adoptă acte de punere în aplicare pentru a specifica procedura tehnică pentru interogarea de către router a bazelor de date ale statelor membre și a datelor Europol, formatul răspunsurilor routerului și normele tehnice de evaluare a corespondenței dintre datele biometrice. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura menționată la articolul 76 alineatul (2).

Articolul 38

Verificarea calității

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

În cazul în care datele sunt necorespunzătoare pentru a se efectua o comparare automată, statul membru solicitat informează fără întârziere statul membru solicitant prin intermediul routerului.

Articolul 39

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

(1) Utilizatorii routerului menționați la articolul 36 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, în cazul în care sunt îndeplinite condițiile relevante prevăzute de dreptul Uniunii și 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 interogărilor se transmite prin intermediul portalului european de căutare.

Numai autoritățile desemnate definite la articolul 4 punctul 20 din Regulamentul (UE) 2019/817 și la articolul 4 punctul 20 din Regulamentul (UE) 2019/818 pot lansa aceste interogări simultane.

Interogările simultane în bazele de date ale statelor membre și în datele Europol și în registrul comun de date de identitate pot fi lansate numai în cazurile în care este probabil ca date privind un suspect, un autor sau o victimă a unei infracțiuni de terorism sau a altor 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, să fie stocate în registrul comun de date de identitate.

Articolul 40

Păstrarea înregistrărilor

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

- (a) statul membru sau agenția Uniunii care a lansat solicitarea de interogare;

- (b) data și ora solicitării;
- (c) data și ora răspunsului;
- (d) bazele de date naționale sau datele Europol cărora le-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 pe care le efectuează autoritățile sale competente și personalul acestor autorități care este 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) pot fi 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.

Aceste înregistrări se protejează prin măsuri corespunzătoare împotriva accesului neautorizat și se șterg după o perioadă de un an 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 este nevoie de ele 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 56.

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, utilizatorii routerului sunt notificați în mod automatizat de eu-LISA. eu-LISA ia măsuri fără întârziere 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 sau în datele Europol din cauza unei defecțiuni a infrastructurii naționale dintr-un stat membru, statul membru respectiv notifică acest lucru celorlalte state membre, eu-LISA și Comisiei în mod automatizat. Statele membre iau măsuri 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 una sau mai multe baze de date naționale sau în datele Europol din cauza unei defecțiuni a infrastructurii Europol, Europol notifică acest lucru statelor membre, eu-LISA și Comisiei în mod automatizat. Europol ia măsuri fără întârziere pentru a soluționa imposibilitatea tehnică de a utiliza routerul.

SECȚIUNEA 2

EPRIS

Articolul 42

EPRIS

(1) Pentru căutarea automatizată a cazierelor judiciare menționate la articolul 26, statele membre și Europol utilizează Sistemul european de inventariere a cazierelor judiciare (EPRIS).

(2) EPRIS este alcătuit din:

- (a) o infrastructură centrală, care include un instrument de căutare care permite interogarea simultană a bazelor de date ale statelor membre;
- (b) un canal de comunicații securizat între infrastructura centrală a sistemului EPRIS, statele membre și Europol.

Articolul 43

Utilizarea EPRIS

(1) În scopul efectuării de căutări de caziere judiciare prin intermediul EPRIS, se utilizează 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 (pseudonimele);
- (b) cetățenia sau cetățeniile;
- (c) locul și țara nașterii;
- (d) genul.

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

Articolul 44

Interogările

(1) Statele membre și Europol solicită o interogare prin transmiterea datelor menționate la articolul 43.

EPRIS transmite cererea de interogare către bazele de date ale statelor membre cu datele transmise de statul membru solicitant 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 al cazierelor judiciare.

(3) Toate concordanțele rezultate în urma interogării în baza de date a fiecărui stat membru sunt trimise înapoi în mod automatizat sistemului EPRIS.

(4) Lista concordanțelor este returnată statului membru solicitant de către EPRIS. Lista concordanțelor precizează calitatea concordanței, precum și statul membru a cărui bază de date conține date care au condus la concordanța respectivă.

(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 (statelor membre) solicitat(e) o solicitare motivată de acțiune ulterioară cuprinzând eventuale informații suplimentare relevante.

(6) Statul membru (statele membre) solicitat(e) prelucrează aceste solicitări fără întârziere pentru a decide dacă partajează datele stocate în baza lor de date.

După confirmare, statul membru (statele membre) solicitat(e) partajează datele menționate la articolul 43, în cazul în care sunt disponibile. Acest schimb de informații se realizează prin intermediul SIENA.

(7) Comisia adoptă acte de punere în aplicare pentru a specifica procedura tehnică pentru interogarea EPRIS în bazele de date ale statelor membre și formatul răspunsurilor. Respectivile acte de punere în aplicare se adoptă în conformitate cu procedura menționată la articolul 76 alineatul (2).

Articolul 45

Păstrarea înregistrărilor

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

- (a) statul membru sau agenția Uniunii care a lansat solicitarea de interogare;
- (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 păstrează înregistrări ale interogărilor efectuate de autoritățile sale competente și de personalul acestora 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 a se monitoriza protecția datelor, inclusiv pentru a se verifica admisibilitatea unei interogări și legalitatea prelucrării datelor, precum și pentru a se asigura securitatea și integritatea datelor.

Aceste înregistrări se protejează prin măsuri corespunzătoare împotriva accesului neautorizat și se șterg după o perioadă de un an 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 este nevoie de ele 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 56.

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 una sau mai multe baze de date naționale 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 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 Europol și Comisiei 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

Schimbul de date de bază

În cazul în care procedurile menționate la articolele 6, 7, 13 sau 22 indică o concordanță între datele utilizate pentru căutare sau comparare și datele deținute în baza de date a statului membru (statelor membre) solicitat(e) și după confirmarea concordanței de către statul membru solicitant, statul membru solicitat returnează prin router un set de date de bază în termen de 24 de ore. Acest set de date de bază, dacă este disponibil, conține următoarele date:

- (a) prenumele;
- (b) numele;
- (c) data nașterii;
- (d) cetățenia sau cetățeniile;
- (e) locul și țara nașterii;
- (f) genul.

Utilizarea SIENA

Orice schimb de date între autoritățile competente ale statelor membre sau cu Europol care nu este prevăzut în mod explicit în prezentul regulament, în orice etapă a uneia dintre procedurile prevăzute de prezentul regulament, se realizează prin intermediul SIENA.

Articolul 49

Accesul statelor membre la datele biometrice provenite din țări terțe 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 această procedură conduce la o concordanță între datele utilizate pentru căutare și datele Europol, acțiunea ulterioară are loc în conformitate cu Regulamentul (UE) 2016/794.

Articolul 50

Accesul Europol la datele stocate în bazele de date ale statelor membre

- (1) În conformitate cu Regulamentul (UE) 2016/794, Europol are acces la datele stocate de statele membre în bazele lor de date naționale în conformitate cu prezentul regulament.
- (2) Interogările efectuate de Europol pe baza datelor biometrice drept criteriu de căutare se efectuează utilizând routerul.
- (3) Interogările efectuate de Europol pe baza datelor privind înmatricularea vehiculelor drept criteriu de căutare se efectuează utilizând Eucaris.
- (4) Interogările efectuate de Europol pe baza cazierelor judiciare drept criteriu de căutare se efectuează utilizând EPRIS.
- (5) Europol efectuează căutările în conformitate cu alineatul (1) numai atunci când își îndeplinește atribuțiile menționate în Regulamentul (UE) 2016/794.
- (6) În cazul în care procedurile menționate la articolele 6, 7, 13 sau 22 indică o concordanță între datele utilizate pentru căutare sau comparare și datele deținute în baza de date națională a statului membru (statelor membre) solicitat(e), după confirmarea concordanței de către Europol, statul membru solicitat decide dacă returnează prin router un set de date de bază în termen de 24 de ore. Acest set de date de bază, dacă este disponibil, conține următoarele date:
 - (a) prenumele;
 - (b) numele;
 - (c) data nașterii;
 - (d) cetățenia sau cetățeniile;
 - (e) locul și țara nașterii;
 - (f) genul.
- (7) Utilizarea de către Europol a informațiilor obținute în urma unei căutări efectuate în conformitate cu alineatul (1) și a schimbului 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 51

Scopul datelor

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

(2) Prelucrarea datelor furnizate în temeiul articolelor 6, 7, 13, 18 sau 22 de către statul membru care efectuează căutarea sau compararea este permisă doar în următoarele scopuri:

- (a) pentru a stabili dacă între profilurile ADN, datele dactiloscopice, datele privind înmatricularea vehiculelor, imaginile faciale și cazierile judiciare comparate există concordanțe;
- (b) pentru a pregăti și a depune o solicitare de asistență juridică din partea poliției, în cazul în care s-a obținut o concordanță între date;
- (c) pentru a efectua înregistrări în sensul articolelor 40 și 45.

(3) Statul membru solicitant poate prelucra datele care i-au fost furnizate în conformitate cu articolele 6, 7, 13 sau 22 numai în cazul în care acest lucru este necesar în sensul prezentului regulament. Datele furnizate se șterg imediat după compararea datelor sau după răspunsurile automatizate la căutări, cu excepția cazului în care este necesară o prelucrare suplimentară de către statul membru solicitant în scopul prevenirii, depistării și cercetării infracțiunilor.

(4) Datele furnizate în conformitate cu articolul 18 pot fi utilizate de statul membru solicitant numai în cazul în care acest lucru este necesar în sensul prezentului regulament. Datele furnizate se șterg imediat după transmiterea răspunsurilor automatizate la căutări, cu excepția cazului în care este necesară o prelucrare suplimentară pentru înregistrare în conformitate cu articolul 20. Statul membru solicitant utilizează datele primite ca răspuns numai pentru procedura pentru care a fost efectuată căutarea.

Articolul 52

Exactitatea, relevanța și păstrarea datelor

(1) Statele membre asigură exactitatea și relevanța actuală a datelor cu caracter personal. În cazul în care un stat membru solicitat constată că au fost furnizate date incorecte sau date care nu ar fi trebuit furnizate, acest lucru se notifică fără întârziere oricărui stat membru solicitant. Toate statele membre solicitante în cauză sunt obligate să corecteze sau să șteargă datele în consecință. De asemenea, datele cu caracter personal furnizate sunt corectate dacă se constată că sunt incorecte. În cazul în care statul membru solicitant are motive să creadă că datele furnizate sunt incorecte sau ar trebui șterse, statul membru solicitat este informat în acest sens.

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

(3) Datele cu caracter personal furnizate 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 legislația națională a statului membru solicitat, dacă statul membru solicitat a informat statul membru solicitant cu privire la acest termen maxim la momentul furnizării datelor.

În cazul în care există motive să se creadă că ștergerea datelor ar aduce atingere intereselor persoanei vizate, datele sunt blocate în loc să fie șterse. Datele blocate pot fi furnizate sau utilizate doar în scopul care a împiedicat ștergerea lor.

Articolul 53

Persoana împuternicită de operatorul de date

- (1) Agenția eu-LISA este persoana împuternicită de operator în sensul 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 pentru prelucrarea datelor cu caracter personal prin intermediul EPRIS.

Articolul 54

Securitatea prelucrărilor de date

- (1) Europol, eu-LISA și autoritățile statelor membre garantează securitatea prelucrării datelor cu caracter personal care are loc în temeiul prezentului regulament. Europol, eu-LISA și autoritățile statelor membre 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 sistemului EPRIS, precum și a infrastructurii de comunicații aferente acestora.
- (3) În special, eu-LISA și Europol adoptă măsurile necesare cu privire la router și, respectiv, la EPRIS, inclusiv un plan de securitate, un plan de asigurare a continuității activității și un plan de redresare în caz de dezastru, 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 că persoanele autorizate să acceseze routerul și EPRIS au acces numai la datele care fac obiectul autorizației lor de acces, prin utilizarea exclusivă a unor nume de utilizator individuale și a unor coduri de acces confidentiale;
- (h) de a asigura posibilitatea de a verifica și de a stabili care sunt organismele cărora le pot fi transmise 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, în ce moment, de către cine și în ce scop;
- (j) de a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transmiterii acestora către sau din router și EPRIS 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 și a sistemului EPRIS;
- (m) de a monitoriza eficacitatea măsurilor de securitate prevăzute la prezentul alineat și de a lua măsurile organizatorice necesare referitoare la monitorizarea internă, astfel încât să se asigure respectarea dispozițiilor prezentului regulament și să se evalueze măsurile de securitate respective în contextul noilor evoluții tehnologice.

Articolul 55

Incidente de securitate

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

(2) Incidentele de securitate sunt gestionate astfel încât să se asigure un răspuns rapid, eficace și corespunzător.

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

Fără a aduce atingere articolului 34 din Regulamentul (UE) 2016/794, 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.

În cazul unui incident de securitate legat de infrastructura centrală a routerului, eu-LISA 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.

(4) 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.

(5) Informațiile privind un incident de securitate care are sau poate avea un impact asupra funcționării sistemului 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 56

Automonitorizarea

(1) Statele membre și agențiile relevante ale Uniunii se asigură că fiecare autoritate care are dreptul de a utiliza sistemul Prüm II ia măsurile necesare pentru a monitoriza respectarea prezentului regulament și cooperează, dacă este cazul, cu autoritatea națională de supraveghere.

(2) Operatorii de date iau măsurile necesare pentru a monitoriza respectarea dispozițiilor prezentului regulament pe parcursul prelucrării datelor, inclusiv prin verificarea frecventă a înregistrărilor menționate la articolele 40 și 45 și cooperează, dacă este cazul, cu autoritățile de supraveghere și cu Autoritatea Europeană pentru Protecția Datelor.

Articolul 57

Sanctiuni

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 eficace, proporționale și disuasive.

Articolul 58

Sarcina probei

(1) Statele membre iau măsurile necesare pentru a se asigura că persoanele care se consideră discriminate ca urmare a prelucrării sau a schimbului de date cu caracter personal nu suportă sarcina probei. În cazurile în care o persoană consideră că a fost discriminată în cadrul unei comparații automate în contextul prezentului regulament în fața unei instanțe judecătorești sau a unei alte autorități judiciare competente, autoritățile statului membru care au prelucrat datele justifică absența discriminării.

(2) Alineatul (1) nu se aplică în cazul procedurilor penale.

(3) Statele membre nu iau măsuri specifice în sensul alineatului (1) pentru procedurile în cadrul cărora este de competența instanței sau a organului judiciar competent să cerceteze faptele cauzei.

Articolul 59

Răspunderea

Dacă orice nerespectare de către un stat membru a obligațiilor care îi revin în temeiul prezentului regulament provoacă prejudicii routerului sau sistemului EPRIS, răspunderea aparține statului membru respectiv, cu excepția cazului în care eu-LISA, Europol sau un alt stat membru care are obligații în

temeiul prezentului regulament nu a luat măsuri rezonabile pentru a preveni producerea prejudiciului sau pentru a reduce la minimum impactul acestuia.

Articolul 60

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 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. Europol și eu-LISA au posibilitatea de a formula observații înainte de adoptarea rapoartelor.

(2) Agenția 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.

Articolul 61

Cooperarea între 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 și asigură 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 sistemului Prüm II.

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

(3) Comitetul european pentru protecția datelor transmite Parlamentului European, Consiliului, Comisiei, Europol și eu-LISA un raport comun privind activitățile sale desfășurate în temeiul prezentului articol până la [2 ani de la intrarea în funcțiune a routerului și a sistemului EPRIS] și, ulterior, din doi în doi ani. Raportul respectiv include un capitol despre fiecare stat membru, elaborat de autoritatea de supraveghere a statului membru respectiv.

Articolul 62

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

Datele prelucrate în conformitate cu prezentul regulament nu se transferă și nu se pun la dispoziția țărilor terțe sau a organizațiilor internaționale în mod automatizat.

CAPITOLUL 7
RESPONSABILITĂȚI

Articolul 63

Responsabilitățile statelor membre

(1) Fiecare stat membru este responsabil pentru:

- (a) conectarea la infrastructura routerului;
- (b) integrarea sistemelor și infrastructurilor 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 infrastructurilor naționale existente cu EPRIS;
- (f) organizarea, gestionarea, exploatarea și întreținerea infrastructurii 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 naționale 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 sistemului EPRIS de către personalul autorizat din cadrul autorităților naționale 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 sistemului Eucaris de către personalul autorizat din cadrul autorităților naționale 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 a unei concordanțe, astfel cum se menționează la articolul 6 alineatul (3), articolul 7 alineatul (3), articolul 13 alineatul (2), articolul 22 alineatul (2) și articolul 26 alineatul (2);
- (k) asigurarea disponibilității datelor necesare pentru schimbul de date în conformitate cu articolele 6, 7, 13, 18, 22 și 26;
- (l) schimbul de informații în conformitate cu articolele 6, 7, 13, 18, 22 și 26;
- (m) 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 cu caracter personal 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 naționale competente la router, la EPRIS și la Eucaris.

Responsabilitățile Europol

- (1) Europol este responsabil pentru gestionarea accesului și modalitățile de accesare a routerului, a sistemului EPRIS și a sistemului Eucaris de către personalul său autorizat în mod corespunzător, în conformitate cu prezentul regulament.
- (2) Europol este, de asemenea, responsabil pentru prelucrarea interogărilor în datele Europol de către router. Acesta 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) Europol este responsabil pentru dezvoltarea sistemului EPRIS în cooperare cu statele membre. EPRIS oferă funcționalitățile prevăzute la articolele 42-46.

Europol asigură 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 efectuarea de interogări în bazele de date naționale în conformitate cu specificațiile tehnice.

- (5) Europol asigură formarea pentru utilizarea tehnică a EPRIS.
- (6) Europol este responsabil pentru procedurile menționate la articolele 49 și 50.

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

- (1) Agenția 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 66 alineatul (1).
- (3) Agenția eu-LISA este responsabilă pentru dezvoltarea routerului și pentru orice adaptări tehnice necesare pentru funcționarea routerului.

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

eu-LISA definește modul în care este concepută arhitectura fizică a routerului, inclusiv a infrastructurilor sale de comunicații, precum și specificațiile tehnice și evoluția acestora în ceea ce privește infrastructura centrală și infrastructura de comunicații securizată. Acest mod de concepere este adoptat de Consiliul de administrație, 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.

eu-LISA dezvoltă și implementează routerul cât mai curând posibil după adoptarea de către Comisie a măsurilor prevăzute la articolul 37 alineatul (6).

Dezvoltarea constă în elaborarea și implementarea specificațiilor tehnice, efectuarea de teste și gestionarea și coordonarea generală a proiectului.

(4) În cursul etapei de concepere și dezvoltare, Consiliul de administrație al programului de interoperabilitate 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 de interoperabilitate prezintă lunar Consiliului de administrație al eu-LISA rapoarte scrise privind evoluția proiectului. Consiliul de administrație al programului de interoperabilitate nu are competențe decizionale și nu dispune de un mandat pentru a-i reprezenta pe membrii Consiliului de administrație al eu-LISA.

Grupul consultativ menționat la articolul 77 se reunește cu regularitate până la începerea funcționării routerului. După fiecare reuniune, acesta prezintă un raport Consiliului de administrație al programului de interoperabilitate. Grupul consultativ pune la dispoziție expertiza tehnică necesară în sprijinul atribuțiilor care îi revin Consiliului de administrație al programului de interoperabilitate și monitorizează stadiul de pregătire al statelor membre.

Articolul 66

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 acesteia 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, disponibilitatea deplină și neîntreruptă a routerului, 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 Consiliului⁴², 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 componentele de interoperabilitate. 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.

⁴² JO L 56, 4.3.1968, p. 1.

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

CAPITOLUL 8

MODIFICAREA ALTOR INSTRUMENTE EXISTENTE

Articolul 67

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

1. În Decizia 2008/615/JAI, 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, astfel cum se prevede la articolul 74.

Prin urmare, 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, astfel cum se prevede la articolul 74.

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, astfel cum se prevede la articolul 74.

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, astfel cum se prevede la articolul 74.

Articolul 68

Modificarea Regulamentului (UE) 2018/1726

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

- (1) Se introduce următorul articol 13a:

„Articolul 13a

Atribuții legate de router

În legătură cu Regulamentul (UE) .../... al Parlamentului European și al Consiliului* [*prezentul regulament*], agenția îndeplinește atribuțiile legate de router care îi sunt conferite prin regulamentul respectiv.

* Regulamentul (UE) [numărul] al Parlamentului European și al Consiliului din xy privind [titlul adoptat oficial] (JO L ...)”

La articolul 17, alineatul (3) se înlocuiește cu următorul text:

„(3) Sediul agenției se află la Tallinn, în Estonia.

Atribuțiile legate de dezvoltarea și gestionarea operațională menționate la articolul 1 alineatele (4) și (5), la articolele 3-8 și la articolele 9, 11 și 13a sunt îndeplinite la amplasamentul tehnic de la Strasbourg, Franța.

Un amplasament de rezervă capabil să asigure funcționarea unui sistem informatic la scară largă în caz de defecțiune a unui astfel de sistem este situat în Sankt Johann im Pongau, Austria.”

Articolul 69

Modificarea Regulamentului (UE) 2019/817

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

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

* Regulamentul (UE) [numărul] al Parlamentului European și al Consiliului din xy privind [titlul adoptat oficial] (JO L ...)”

Articolul 70

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):

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

* Regulamentul (UE) [numărul] al Parlamentului European și al Consiliului din xy privind [titlul adoptat oficial] (JO L ...)”

(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, 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 scop operațional, de elaborare a politicilor și de asigurare a calității datelor. CRRS sprijină, de asemenea, obiectivele Prüm II.”

„(2) Agenția 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 de sistemul de informații al UE. De asemenea, eu-LISA colectează datele și statisticile de la routerul menționat la articolul 65 alineatul (1) din Regulamentul (UE) ... /...* [*prezentul regulament*]. 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 65 alineatul (1) din Regulamentul (UE) .../...* [prezentul regulament].”

CAPITOLUL 9

DISPOZIȚII FINALE

Articolul 71

Raportare și statistici

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

- (a) numărul de interogări pentru fiecare stat membru și pentru Europol;
- (b) numărul de interogări pentru fiecare categorie de date;
- (c) numărul de interogări în fiecare dintre bazele de date conectate;
- (d) numărul de concordanțe cu baza de date a fiecărui stat membru pentru fiecare categorie de date;
- (e) numărul de concordanțe cu datele Europol pentru fiecare categorie de date;
- (f) numărul de concordanțe confirmate în cazul cărora au avut loc schimburi de date de bază și
- (g) numărul de interogări în registrul comun de date de identitate prin router.

Datele trebuie să nu permită identificarea persoanelor.

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

- (a) numărul de interogări pentru fiecare stat membru și 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 trebuie să nu permită identificarea persoanelor.

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

- (a) numărul de interogări pentru fiecare stat membru și 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 trebuie să nu permită identificarea persoanelor.

(4) Agenția eu-LISA stochează datele menționate la alineatele respective.

Datele permit autorităților menționate la alineatul (1) să obțină rapoarte și statistici adaptabile pentru a spori eficiența cooperării în materie de asigurare a respectării legii.

Articolul 72

Costuri

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

(2) Costurile aferente integrării infrastructurilor naționale existente și conexiunile acestora cu routerul și EPRIS, precum și costurile suportate în legătură cu crearea bazelor de date naționale cu imagini faciale și a registrelor naționale ale poliției pentru prevenirea, depistarea și cercetarea 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 programului informatic Eucaris menționat la articolul 19 alineatul (1).

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

Articolul 73

Notificări

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

(2) Agenția eu-LISA notifică Comisiei finalizarea cu succes a testării menționate la articolul 74 alineatul (1) litera (b).

(3) Statele membre notifică Comisiei, Europol și eu-LISA punctele naționale de contact.

Articolul 74

Începerea funcționării

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

- (a) măsurile prevăzute 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 statelor membre și cu Europol.

În respectivul act de punere în aplicare, Comisia stabilește, de asemenea, data de la care statele membre și agențiile Uniunii trebuie să înceapă să utilizeze routerul. Această 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 agențiile Uniunii trebuie să înceapă să utilizeze routerul, în cazul în care o evaluare a implementării routerului a indicat că o astfel de amânare este necesară. Aceste acte de punere în aplicare se adoptă în conformitate cu procedura menționată la articolul 76 alineatul (2).

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

- (a) măsurile prevăzute la articolul 44 alineatul (7) 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 statelor membre.

(3) 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 49, după îndeplinirea următoarelor condiții:

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

(4) 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 50, după îndeplinirea următoarelor condiții:

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

Articolul 75

Dispoziții tranzitorii și derogări

(1) Statele membre și agențiile Uniunii încep să aplice articolele 21-24, articolul 47 și articolul 50 alineatul (6) de la data stabilită în conformitate cu articolul 74 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 50 alineatul (4) de la data stabilită în conformitate cu articolul 74 alineatul (2).

(3) Statele membre și agențiile Uniunii încep să aplice articolul 49 de la data stabilită în conformitate cu articolul 74 alineatul (3).

(4) Statele membre și agențiile Uniunii încep să aplice articolul 50 alineatele (1), (2), (3), (5) și (7) de la data stabilită în conformitate cu articolul 74 alineatul (4).

Articolul 76

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 avis, 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 77

Grupul consultativ

Responsabilitățile Grupului consultativ pentru interoperabilitate al eu-LISA 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 78

Manual practic

Comisia, în strânsă cooperare cu statele membre, cu Europol și cu eu-LISA, 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 sub forma unei recomandări.

Articolul 79

Monitorizare și evaluare

(1) Agenția eu-LISA și, respectiv, Europol se asigură că există proceduri pentru a monitoriza dezvoltarea routerului și a sistemului EPRIS din perspectiva obiectivelor legate de planificare și costuri și pentru a monitoriza funcționarea routerului și a EPRIS din perspectiva obiectivelor legate de realizările tehnice, raportul cost/eficacitate, securitate și calitatea serviciilor.

(2) Până la [un an de la intrarea în vigoare a prezentului regulament] și, ulterior, în fiecare an în cursul etapei de dezvoltare a routerului, eu-LISA prezintă Parlamentului European și, respectiv, Consiliului un raport privind stadiul dezvoltării routerului. Respectivul raport conține informații detaliate despre costurile implicate, precum și informații despre riscurile care pot avea un impact asupra costurilor totale care urmează a fi suportate din bugetul general al Uniunii, în conformitate cu articolul 72.

După încheierea etapei de dezvoltare a routerului, eu-LISA transmite Parlamentului European și Consiliului un raport în care se 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 [un an de la intrarea în vigoare a prezentului regulament] și, ulterior, în fiecare an în cursul etapei de dezvoltare a EPRIS, Europol prezintă Parlamentului European și Consiliului un raport privind stadiul pregătirilor pentru punerea în aplicare a prezentului regulament și stadiul dezvoltării EPRIS, inclusiv informații detaliate cu privire la costurile suportate și informații despre riscurile care ar putea avea un impact asupra costurilor totale care urmează să fie suportate din bugetul general al Uniunii, în conformitate cu articolul 72.

După încheierea etapei de dezvoltare a EPRIS, Europol transmite Parlamentului European și Consiliului un raport în care se 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 și Europol au acces la informațiile necesare referitoare la operațiunile de prelucrare a datelor efectuate în router și, respectiv, 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 acestuia.

(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 acestuia.

(7) După trei ani de la punerea în funcțiune a routerului și a sistemului EPRIS, astfel cum se prevede la articolul 74 și, ulterior, o dată la patru ani, Comisia realizează o evaluare generală a cadrului Prüm II, inclusiv:

- (a) o analiză a aplicării prezentului regulament;
- (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 Prüm II și ale practicilor sale de lucru având în vedere obiectivele, mandatul și atribuțiile sale;
- (d) o evaluare a gradului de securitate al sistemului Prüm II.

Comisia transmite raportul de evaluare Parlamentului European, Consiliului, Autorității Europene pentru Protecția Datelor și Agenției pentru Drepturi Fundamentale a Uniunii Europene.

(8) Statele membre și Europol furnizează agenției eu-LISA și Comisiei informațiile necesare pentru elaborarea rapoartelor menționate la alineatele (2) și (5). Aceste informații nu afectează metodele de lucru și nici nu includ date care dezvăluie sursele, membrii personalului sau cercetările autorităților desemnate.

(9) Statele membre transmit Europol și Comisiei informațiile necesare pentru elaborarea rapoartelor prevăzute la alineatele (3) și (6). Aceste informații nu afectează metodele de lucru și nici nu includ date care dezvăluie sursele, membrii personalului sau cercetările autorităților desemnate.

(10) Statele membre, eu-LISA și Europol furnizează Comisiei informațiile necesare pentru realizarea evaluărilor 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 de date.

Articolul 80

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 Bruxelles,

*Pentru Parlamentul European,
Președintele*

*Pentru Consiliu,
Președintele*

FIȘA FINANCIARĂ LEGISLATIVĂ

1. CADRUL INIȚIATIVEI LEGISLATIVE

1.1. Titlul inițiativei legislative

Propunere de regulament al Parlamentului European și al Consiliului privind schimbul automatizat de date în scopul cooperării polițienești („Prüm II”), de modificare a Deciziilor 2008/615/JAI și 2008/616/JAI ale Consiliului și a Regulamentelor (UE) 2018/1726, 2019/817 și 2019/818 ale Parlamentului European și ale Consiliului

1.2. Domeniul (domeniile) de politică vizat(e)

Domeniul de politică: Afaceri interne

Activitatea: Securitate

1.3. Propunerea se referă la

☐ o acțiune nouă

☐ o acțiune nouă întreprinsă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare⁴³

☒ prelungirea unei acțiuni existente

☐ o fuziune a uneia sau mai multor acțiuni într-o altă/o nouă acțiune

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) general(e)

Ca răspuns la nevoile operaționale presante și la solicitările Consiliului de a examina posibilitatea revizuirii Deciziilor Prüm⁴⁴ în vederea extinderii domeniului lor de aplicare și a actualizării cerințelor tehnice și juridice necesare, se preconizează că prezenta inițiativă va consolida schimburile automatizate de date în temeiul cadrului Prüm pentru a ajuta autoritățile de aplicare a legii din statele membre să combată criminalitatea.

1.4.2. Obiectiv(e) specific(e)

Inițiativa urmărește să atingă următoarele obiective:

1) **Obiectivul specific I:** Furnizarea unei soluții tehnice pentru ca autoritățile de aplicare a legii din UE să poată face schimburi automatizate eficiente de date, astfel încât acestea să aibă acces la datele relevante care sunt disponibile în baza de date națională a unui alt stat membru;

2) **Obiectivul specific II:** Asigurarea disponibilității – pentru toate autoritățile competente de aplicare a legii din UE – a unor date mai relevante (și anume imagini faciale și caziere judiciare) din bazele de date naționale ale altor state membre;

3) **Obiectivul specific III:** Asigurarea disponibilității – pentru autoritățile naționale de aplicare a legii – a datelor relevante (din punctul de vedere al surselor de date) din baza de date a Europol și asigurarea utilizării de către Europol a datelor sale la întregul potențial;

⁴³ Astfel cum se menționează la articolul 58 alineatul (2) litera (a) sau (b) din Regulamentul financiar.

⁴⁴ Deciziile 2008/615/JAI și 2008/616/JAI ale Consiliului.

4) **Obiectivul specific IV:** Asigurarea – pentru autoritățile de aplicare a legii – a unui acces eficient la datele efective corespunzătoare unui rezultat pozitiv care sunt disponibile în baza de date națională a unui alt stat membru sau la nivelul Europol.

1.4.3. Rezultatul (rezultatele) și impactul preconizate

A se preciza efectele pe care ar trebui să le aibă inițiativa legislativă asupra beneficiarilor vizati/grupurilor vizate.

Inițiativa va remedia în mod eficace problemele identificate și va consolida actualul cadru Prüm cu capacități suplimentare specifice și puternice pentru a intensifica sprijinul acordat statelor membre în ceea ce privește consolidarea schimbului de informații, având ca obiectiv final prevenirea și cercetarea infracțiunilor și a actelor de terorism, cu respectarea deplină a drepturilor fundamentale.

Beneficiarii finali ai tuturor opțiunilor preferate sunt **cetățenii**, care vor beneficia în mod direct și indirect de **consolidarea luptei împotriva criminalității și de scăderea ratei criminalității**. În ceea ce privește eficiența, principalii beneficiari sunt **autoritățile naționale de aplicare a legii**. Inițiativa prevede soluții eficiente la provocări care, în caz contrar, ar trebui abordate cu costuri mai ridicate sau cu o eficiență mai redusă.

1.4.4. Indicatorii de performanță

A se preciza indicatorii care permit monitorizarea progreselor și a realizărilor obținute.

Dezvoltarea routerului și a EPRIS va începe după îndeplinirea condițiilor prealabile, și anume adoptarea propunerii legislative de către colegiitori și îndeplinirea condițiilor tehnice prealabile. În timp ce lucrările privind routerul încep ca un nou proiect, lucrările privind EPRIS ar trebui să se bazeze pe actualul proiect ADEP.EPRIS.

Obiectiv specific: sistemul să fie funcțional până la data-limită stabilită

Până în 2023, propunerea se trimite colegiitorilor în vederea adoptării. Prin analogie cu timpul necesar adoptării altor propuneri, se preconizează că procesul de adoptare va fi finalizat în cursul anului 2024.

În această ipoteză, demararea perioadei de dezvoltare este fixată la începutul anului 2025 (=T0); va exista astfel un punct de referință, nu date absolute, de la care se vor calcula perioadele. În cazul în care colegiitorii adoptă proiectul la o dată ulterioară, calendarul se modifică în consecință.

Se preconizează că dezvoltarea routerului și a EPRIS va avea loc în 2025 și 2026, începerea funcționării fiind planificată în 2027.

Următorii indicatori principali vor permite monitorizarea punerii în aplicare și a performanței obiectivelor specifice:

Obiectivul specific I: Furnizarea unei soluții tehnice pentru schimbul automatizat eficient de date.

– Numărul de cazuri de utilizare executate (= numărul de solicitări de interogări care pot fi gestionate de router) într-o anumită perioadă.

– Numărul de cazuri de utilizare executate (= numărul de solicitări de interogări care pot fi gestionate de EPRIS) într-o anumită perioadă.

Obiectivul specific II: Asigurarea disponibilității unor date mai relevante

– Numărul de solicitări de interogare referitoare la imagini faciale

– Numărul de solicitări de interogare referitoare la caziere judiciare

– Numărul de concordanțe în urma interogărilor referitoare la imagini faciale

- Numărul de concordanțe în urma interogărilor referitoare la caziere judiciare

Obiectivul specific III: Asigurarea disponibilității – pentru autoritățile naționale de aplicare a legii – a datelor relevante (din punctul de vedere al surselor de date) din baza de date a Europol și asigurarea utilizării de către Europol a datelor sale la întregul potențial.

- Numărul de solicitări de interogare referitoare la date biometrice ale Europol provenite din țări terțe

- Numărul de concordanțe cu datele biometrice ale Europol provenite din țări terțe
- Numărul de solicitări de interogare emise de Europol
- Numărul de concordanțe rezultate în urma interogărilor efectuate de Europol

Obiectivul specific IV: Asigurarea – pentru autoritățile de aplicare a legii – a unui acces eficient la datele efective corespunzătoare unui rezultat pozitiv care sunt disponibile în baza de date națională a unui alt stat membru sau la nivelul Europol.

- Numărul de concordanțe în urma solicitărilor de interogări comparativ cu numărul de solicitări de schimb de date de bază

1.5. Temeiurile inițiativei legislative

1.5.1. *Cerința (cerințele) care trebuie îndeplinită (îndeplinite) pe termen scurt sau lung, inclusiv un calendar detaliat pentru punerea în aplicare a inițiativei legislative*

Punerea în aplicare a inițiativei legislative necesită măsuri tehnice și procedurale la nivelul UE și la nivel național, care ar trebui să înceapă să se aplice odată cu intrarea în vigoare a legislației revizuite. Resursele relevante – în special resursele umane – ar trebui sporite în timp, în conformitate cu măsurile.

Principalele cerințe care trebuie îndeplinite în urma intrării în vigoare a propunerii sunt următoarele:

Pentru crearea routerului Prüm:

îndeplinirea obiectivului de a le oferi utilizatorilor sistemului Prüm II o conexiune unică la bazele de date ale tuturor statelor membre și la datele Europol pentru a trimite solicitări de interogare referitoare la date biometrice.

Punerea la dispoziție a unei noi acțiuni ulterioare la nivelul UE, cu un schimb semiautomatizat de date reale corespunzătoare unui rezultat pozitiv.

Pentru crearea/extinderea EPRIS:

îndeplinirea obiectivului de a le oferi utilizatorilor sistemului Prüm II o conexiune unică la bazele de date ale tuturor statelor membre participante care conțin caziere judiciare pentru a trimite solicitări de interogare referitoare la caziere judiciare.

Pentru a permite statelor membre să facă schimb de noi categorii de date:

Posibilitatea schimbului de imagini faciale și de caziere judiciare prin intermediul sistemului Prüm II.

Pentru a permite statelor membre să verifice în mod automat datele provenite din țări terțe de la nivelul Europol, ca parte a cadrului Prüm:

Posibilitatea verificării de către statele membre a datelor biometrice provenite din țări terțe prin intermediul sistemului Prüm II.

Pentru a permite Europol să verifice datele provenite din țări terțe în bazele de date naționale ale statelor membre:

Posibilitatea utilizării de către Europol a datelor provenite din țări terțe pentru a efectua căutări în bazele de date ale statelor membre prin intermediul sistemului Prüm II.

Întrucât toate obiectivele trebuie îndeplinite, soluția completă constă într-o combinație a celor de mai sus.

- 1.5.2. *Valoarea adăugată a intervenției Uniunii (aceasta poate rezulta din diferiți factori, de exemplu o mai bună coordonare, securitate juridică, o mai mare eficacitate sau complementaritate). În sensul prezentului punct, „valoarea adăugată a intervenției Uniunii” este valoarea rezultată din intervenția Uniunii care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre.*

Formele grave de criminalitate și terorismul au un caracter transnațional. Prin urmare, acestea nu pot fi contracarate în mod eficace doar prin luarea de măsuri la nivel național. Din acest motiv, statele membre aleg să colaboreze în cadrul UE pentru a combate amenințările pe care le reprezintă formele grave de criminalitate și terorismul.

În plus, amenințările în permanentă evoluție la adresa securității, determinate de diferitele moduri în care infractorii exploatează avantajele oferite de transformarea digitală, globalizare și mobilitate, impun, de asemenea, ca UE să sprijine activitatea autorităților naționale de aplicare a legii. Intervenția UE oferă o modalitate eficace și eficientă de a intensifica sprijinul acordat statelor membre în combaterea formelor grave de criminalitate și a terorismului pentru a face față acestor amenințări în permanentă evoluție.

Propunerea va crea economii de scară semnificative prin transferarea sarcinilor și a serviciilor care pot fi îndeplinite mai eficient la nivelul UE, de la nivel național la Europol. Prin urmare, propunerea prevede soluții eficiente la provocări care, în caz contrar, ar trebui abordate cu costuri mai ridicate, prin intermediul a 27 de soluții naționale individuale, sau la provocări care nu pot fi abordate deloc la nivel național, dat fiind caracterul lor transnațional.

- 1.5.3. *Învățămintele desprinse din experiențele anterioare similare*

Evaluarea Deciziilor Prüm a arătat că:

- Cadrul Prüm este relevant, având în vedere nevoile și provocările actuale și viitoare legate de securitate și, mai precis, de cercetările penale. Cooperarea și schimbul de informații între autoritățile de aplicare a legii din statele membre, precum și posibilitatea de a căuta și a compara date ADN, date dactiloscopice și date privind înmatricularea vehiculelor în bazele de date ale altor state membre în vederea prevenirii și cercetării infracțiunilor sunt considerate a fi de o importanță capitală pentru garantarea securității interne a UE și a siguranței cetățenilor săi.
- Din perspectiva categoriilor de date care sunt disponibile, conceptul care stă la baza Deciziilor Prüm răspunde nevoilor anchetatorilor în materie penală, ale victimelor criminalității, ale specialiștilor criminaliști, ale custozilor de baze de date și ale practicienilor din domeniul dreptului.

- Prin prevenirea necesității de a efectua interogări bilaterale în fiecare stat membru, schimbul automatizat de date în temeiul cadrului Prüm aduce creșteri de eficiență în ceea ce privește schimbul de informații în materie de asigurare a respectării legii, îmbunătățind viteza schimburilor și reducând sarcina administrativă într-o anumită măsură. S-a constatat că aceste beneficii depășesc investițiile necesare pentru punerea în aplicare a cadrului Prüm. În plus, sistemul Prüm automatizat asigură economii substanțiale în ceea ce privește timpul de lucru. Totuși, există în continuare o sarcină administrativă generată de verificarea rezultatelor pozitive și de raportare, precum și de primirea/transmiterea informațiilor din a doua etapă.
- De asemenea, de la adoptarea Deciziilor Prüm în 2008 s-au produs evoluții și schimbări considerabile în ceea ce privește cadrul juridic al UE, nevoile operaționale și posibilitățile tehnice și criminalistice. S-au dezvoltat mai multe inițiative și sisteme la nivelul UE și la nivel internațional care vizează facilitarea schimbului de informații între autoritățile de aplicare a legii. Există, în cea mai mare parte, complementarități între Deciziile Prüm și alte acte legislative relevante ale UE/internaționale, inclusiv cadrul de interoperabilitate. De asemenea, există complementarități cu unele dintre sistemele centrale de informații ale UE care au scopuri diferite. Pot fi identificate sinergii potențiale în ceea ce privește Europol și cadrul de interoperabilitate.
- Cu toate acestea, punerea în aplicare a Deciziilor Prüm a fost lentă. După aproape zece ani de la termenul-limită pentru punerea în aplicare, 26 august 2011, nu toate statele membre au finalizat procedura de evaluare și o serie de conexiuni bilaterale nu se pot stabili din cauza complexității tehnice și a resurselor financiare și umane importante pe care le implică. În consecință, interogările nu pot fi verificate în raport cu datele din unele state membre cu care conexiunea bilaterală relevantă nu se poate stabili. Acest lucru afectează capacitatea de identificare a infractorilor și de detectare a legăturilor transfrontaliere dintre infracțiuni, ceea ce împiedică schimbul de informații și funcționarea sistemului Prüm.
- Faptul că acțiunile ulterioare rezultatelor pozitive obținute în temeiul cadrului Prüm au loc în conformitate cu dreptul intern și, prin urmare, în afara domeniului de aplicare al Deciziilor Prüm a fost, de asemenea, semnalat ca o chestiune care împiedică funcționarea sistemului Prüm. Într-adevăr, din cauza diferențelor dintre normele și procedurile naționale, schimbul de date ca urmare a rezultatelor pozitive este fragmentat, fiind nevoie uneori de săptămâni sau chiar luni pentru a primi informațiile relevante care au generat un rezultat pozitiv.

1.5.4. *Compatibilitatea cu cadrul financiar multianual și posibilele sinergii cu alte instrumente corespunzătoare*

Investițiile necesare la nivelul UE sunt compatibile cu cadrul financiar multianual 2021-2027, finanțarea încadrându-se la rubrica Securitate și apărare și la rubrica Migrație și frontiere.

1.5.5. *Evaluarea diferitelor opțiuni de finanțare disponibile, inclusiv a posibilităților de realocare a creditelor*

Creditele necesare pentru finanțarea dezvoltării cadrului Prüm II nu au fost planificate în cadrul alocărilor CFM pentru Europol și eu-LISA, deoarece aceasta este o propunere nouă, pentru care sumele nu erau cunoscute la momentul propunerii. Se propune creșterea alocărilor pentru Europol și eu-LISA în anii 2024, 2025, 2026 și 2027 prin reduceri corespunzătoare ale Fondului pentru securitate internă (FSI) și, respectiv, ale Instrumentului pentru gestionarea frontierelor și vize (IGFV).

1.6. Durata și impactul financiar al inițiativei legislative

☐ durată limitată

☐ Propunere/inițiativă în vigoare din [ZZ/LL]AAAA până în [ZZ/LL]AAAA

☐ Impact financiar din AAAA până în AAAA

☒ durată nelimitată

Punere în aplicare cu o perioadă de creștere în intensitate din 2024 până în 2026 urmată de o perioadă de funcționare la capacitate maximă.

1.7. Modul (modurile) de gestiune preconizat(e)⁴⁵

☒ Gestiune directă asigurată de Comisie

– X prin serviciile sale, inclusiv prin intermediul personalului din delegațiile Uniunii;

– ☐ de agențiile executive

☒ Gestiune partajată cu statele membre

☒ Gestiune indirectă, cu delegarea sarcinilor de execuție bugetară:

☐ organizațiilor internaționale și agențiilor acestora (a se preciza);

☐ BEI și Fondului european de investiții;

☒ organismelor menționate la articolele 70 și 71;

☐ organismelor de drept public;

☐ organismelor de drept privat cu misiune de serviciu public, cu condiția să prezinte garanții financiare adecvate;

☐ organismelor de drept privat dintr-un stat membru care sunt responsabile cu punerea în aplicare a unui parteneriat public-privat și care prezintă garanții financiare adecvate;

☐ persoanelor cărora li se încredințează executarea unor acțiuni specifice în cadrul PESC, în temeiul titlului V din TUE, și care sunt identificate în actul de bază relevant.

Observații

Blocuri	Etapă de dezvoltare	Etapă de funcționare	Mod de gestiune	Actori
Dezvoltare și întreținere (a routerului și a EPRIS)	X	X	Indirectă	eu-LISA Europol
Adaptarea bazelor de date ale Europol	X	X	Indirectă	Europol

⁴⁵ Explicații detaliate privind modurile de gestiune și trimerile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: <https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>.

Blocuri	Etapă de dezvoltare	Etapă de funcționare	Mod de gestiune	Actori
Dezvoltarea sau îmbunătățirea bazelor de date naționale existente, integrarea sistemelor naționale	X	X	Partajată (sau directă)	COM + Statele membre

Perioada de dezvoltare începe în 2024 și durează până la realizarea fiecărei părți a inițiativei, între 2024 și 2027.

(1) Gestiune directă asigurată de DG HOME: În perioada de dezvoltare, dacă este necesar, acțiunile pot fi puse în aplicare și direct de către Comisie. Acest lucru ar putea include, în special, sprijin financiar oferit de Uniune pentru activități sub formă de granturi (acordate inclusiv autorităților naționale ale statelor membre), contracte de achiziții publice și/sau rambursarea cheltuielilor suportate de experții externi.

(2) Gestiune partajată: În cursul etapei de dezvoltare, statele membre vor trebui să își adapteze sistemele naționale pentru a se conecta la router și la EPRIS și să prevadă măsurile necesare pentru a asigura schimbul de imagini faciale și de cazier judiciar.

(3) Gestiune indirectă: eu-LISA și Europol vor asigura partea de dezvoltare a componentelor informatice ale proiectului, și anume routerul și, respectiv, EPRIS. Aceasta ar include orice modificare necesară a arhitecturii lor existente pentru a asigura capacitățile descrise în propunere.

Pe durata funcționării, eu-LISA și Europol vor executa toate activitățile tehnice legate de întreținerea routerului și, respectiv, a EPRIS.

Europol va asigura dezvoltarea și întreținerea sistemelor sale pentru a garanta că datele sale sunt disponibile în contextul cadrului Prüm.

(2) MĂSURI DE GESTIUNE

2.1. Norme privind monitorizarea și raportarea

A se preciza frecvența și condițiile aferente monitorizării și raportării.

Agencia eu-LISA și, respectiv, Europol se asigură că există proceduri pentru a monitoriza dezvoltarea routerului și a sistemului EPRIS din perspectiva obiectivelor legate de planificare și costuri și pentru a monitoriza funcționarea routerului și a EPRIS din perspectiva obiectivelor legate de realizările tehnice, de raportul cost/eficacitate, de securitate și de calitatea serviciilor.

În termen de cel mult un an de la adoptarea regulamentului propus și, ulterior, în fiecare an în cursul etapei de dezvoltare a routerului, eu-LISA prezintă Parlamentului European și Consiliului un raport privind stadiul dezvoltării routerului. Raportul conține informații detaliate despre costurile implicate, precum și informații despre riscurile care pot avea un impact asupra costurilor totale care urmează a fi suportate din bugetul general al Uniunii.

După încheierea etapei de dezvoltare a routerului, eu-LISA transmite Parlamentului European și Consiliului un raport în care se 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.

În termen de cel mult un an de la intrarea în vigoare a regulamentului propus și, ulterior, în fiecare an în cursul etapei de dezvoltare a EPRIS, Europol prezintă Parlamentului European și Consiliului un raport privind stadiul pregătirilor pentru punerea în aplicare a prezentului regulament și stadiul dezvoltării EPRIS, inclusiv informații detaliate cu privire la costurile suportate și informații despre riscurile care ar putea avea un impact asupra costurilor totale care urmează să fie suportate din bugetul general al Uniunii.

După încheierea etapei de dezvoltare a EPRIS, Europol transmite Parlamentului European și Consiliului un raport în care se 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.

Pentru asigurarea întreținerii tehnice, eu-LISA și Europol au acces la informațiile necesare referitoare la operațiunile de prelucrare a datelor efectuate în router și, respectiv, în EPRIS.

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 acestuia.

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 acestuia.

După trei ani de la punerea în funcțiune a tuturor elementelor regulamentului propus și, ulterior, o dată la patru ani, Comisia realizează o evaluare generală a Prüm II, inclusiv:

- (a) o analiză a aplicării prezentului regulament;
- (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 Prüm II și ale practicilor sale de lucru având în vedere obiectivele, mandatul și atribuțiile sale;
- (d) o evaluare a gradului de securitate al sistemului Prüm II.

Comisia transmite raportul de evaluare Parlamentului European, Consiliului, Autorității Europene pentru Protecția Datelor și Agenției pentru Drepturi Fundamentale a Uniunii Europene.

Statele membre și Europol furnizează eu-LISA și Comisiei informațiile necesare pentru elaborarea rapoartelor menționate anterior. Aceste informații nu afectează metodele de lucru și nici nu includ date care dezvăluie sursele, membrii personalului sau cercetările autorităților desemnate.

Statele membre furnizează Europol și Comisiei informațiile necesare pentru elaborarea rapoartelor menționate anterior. Aceste informații nu afectează metodele de lucru și nici nu includ date care dezvăluie sursele, membrii personalului sau cercetările autorităților desemnate.

eu-LISA și Europol furnizează Comisiei informațiile necesare pentru realizarea evaluărilor sale.

2.2. Sistemul (sistemele) de gestiune și de control

2.2.1. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor

S-au identificat următoarele riscuri:

- resurse operaționale reduse din cauza creșterii fluxurilor de date și a evoluției constante a situației în materie de activități infracționale;
- multiplicarea sarcinilor și a solicitărilor atât pentru eu-LISA, cât și pentru Europol;
- lipsa unor niveluri adecvate de resurse financiare și umane, care să corespundă nevoilor operaționale;
- lipsa resurselor TIC, care ar genera întârzieri în ceea ce privește dezvoltarea și actualizările sistemului principal;
- riscuri legate de prelucrarea datelor cu caracter personal de către Europol și de necesitatea de a evalua cu regularitate și de a adapta garanțiile procedurale și tehnice pentru a asigura protecția datelor cu caracter personal și a drepturilor fundamentale;
- dependențele dintre pregătirile care trebuie efectuate de eu-LISA în ceea ce privește routerul și pregătirile care trebuie efectuate de statele membre și de Europol în ceea ce privește crearea unei interfețe tehnice pentru transmiterea datelor prin router.

Aceste riscuri pot fi diminuate prin aplicarea unor tehnici de gestionare a proiectelor, printre care se numără intervențiile de urgență în proiectele de dezvoltare și dotarea cu personal suficient pentru absorbirea volumului de muncă excesiv în perioadele de vârf. Într-adevăr, estimarea efortului se efectuează, de obicei, pornind de la premisa unei distribuții uniforme a volumului de muncă în timp, dar, în realitate, proiectele se caracterizează printr-un volum inegal de muncă, care este absorbit printr-o alocare de resurse suplimentare.

Există mai multe riscuri legate de utilizarea unui contractant extern pentru aceste lucrări de dezvoltare, în special:

1. riscul ca respectivul contractant să nu reușească să aloce resurse suficiente proiectului sau să conceapă și să creeze un sistem care să nu corespundă stadiului actual al tehnologiei;
2. riscul ca tehnicile și metodele administrative de gestionare a proiectelor informatice să nu fie pe deplin respectate, în încercarea de a reduce costurile de către contractant;

3. riscul ca respectivul contractant să se confrunte cu dificultăți financiare din motive independente de acest proiect.

Aceste riscuri sunt atenuate prin atribuirea contractelor pe baza unor criterii de calitate solide, prin verificarea referințelor contractanților și prin menținerea unei relații strânse cu aceștia. În cele din urmă, ca ultimă soluție, se pot include și aplica clauze stricte de penalizare și de reziliere, dacă acest lucru este necesar.

Europol pune în aplicare un cadru specific de control intern bazat pe cadrul de control intern al Comisiei Europene și pe cadrul de control intern integrat stabilit inițial de Comitetul Organizațiilor de Sponsorizare. Documentul unic de programare trebuie să furnizeze informații referitoare la sistemele de control intern, în timp ce raportul anual de activitate consolidat trebuie să conțină informații referitoare la eficiența și eficacitatea sistemelor de control intern, inclusiv în ceea ce privește evaluarea riscurilor. Raportul anual de activitate consolidat pentru 2019 menționează că, pe baza analizei componentelor și a principiilor de control intern care au fost monitorizate în cursul anului 2019, utilizând atât elemente cantitative, cât și calitative, sistemul de control intern al Europol este evaluat ca fiind prezent și ca funcționând în mod integrat în cadrul agenției.

Pentru bugetul executat de eu-LISA, este necesar un cadru specific de control intern bazat pe cadrul de control intern al Comisiei Europene. Documentul unic de programare trebuie să furnizeze informații privind sistemele de control intern, în timp ce raportul anual de activitate consolidat trebuie să conțină informații privind eficiența și eficacitatea sistemelor de control intern, inclusiv în ceea ce privește evaluarea riscurilor. Conform raportului anual de activitate consolidat pe 2019, conducerea agenției are certitudinea, în limite rezonabile, că există controale interne adecvate, care funcționează așa cum s-a intenționat. Pe tot parcursul anului, riscurile majore au fost identificate, monitorizate și gestionate în mod corespunzător. Această certitudine este confirmată și de rezultatele auditurilor interne și externe efectuate.

Atât pentru Europol, cât și pentru eu-LISA, un nivel suplimentar de supraveghere internă este asigurat de structura de audit intern a Europol, pe baza unui plan anual de audit, luând în considerare în special evaluarea riscurilor din cadrul Europol. Structura de audit intern ajută Europol să își îndeplinească obiectivele, printr-o abordare sistematică și metodică de evaluare a eficacității proceselor de gestionare a riscurilor, de control și de guvernanță și prin emiterea de recomandări pentru îmbunătățirea acestora.

În plus, Autoritatea Europeană pentru Protecția Datelor (AEPD) și responsabilul cu protecția datelor din cele două agenții (o funcție independentă atașată direct secretariatului Consiliului de administrație) supraveghează prelucrarea datelor cu caracter personal de către agenții.

În fine, în calitate de direcție generală parteneră pentru Europol și eu-LISA, DG HOME efectuează un exercițiu anual de gestionare a riscurilor pentru a identifica și a evalua potențialele riscuri ridicate legate de operațiunile agențiilor. Riscurile considerate critice sunt raportate anual în planul de gestionare al DG HOME și sunt însoțite de un plan de acțiune care precizează acțiunile de atenuare.

2.2.2. *Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul dintre costurile controalelor și valoarea fondurilor aferente gestionate) și evaluarea nivelurilor preconizate ale riscului de eroare (la plată și la închidere)*

Raportul dintre costurile controalelor și valoarea fondurilor aferente gestionate este prezentat de Comisie. Conform raportului anual de activitate pe 2020 al DG HOME, acesta a fost de 0,21 % în cazul entităților cărora le-a fost încredințată gestiunea indirectă și al agențiilor descentralizate, printre care se numără și Europol și eu-LISA.

Curtea de Conturi Europeană a confirmat legalitatea și regularitatea conturilor anuale ale Europol și ale eu-LISA pentru 2019, ceea ce implică o rată de eroare mai mică de 2 %. Nu există indicii conform cărora rata de eroare va crește în următorii ani.

În plus, articolul 80 din Regulamentul financiar al Europol și, respectiv, din Regulamentul financiar al eu-LISA prevede posibilitatea ca agenția să partajeze o structură de audit intern cu alte organisme ale Uniunii care își desfășoară activitatea în același domeniu de politică, în cazul în care capacitatea de audit intern a unui singur organism al Uniunii nu este eficientă din punctul de vedere al costurilor.

2.3. Măsuri de prevenire a fraudelor și a neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate, de exemplu din strategia antifraudă.

Măsurile avute în vedere pentru combaterea fraudei sunt prevăzute la articolul 35 din Regulamentul (UE) nr. 1077/2011.

Măsurile legate de combaterea fraudei, a corupției și a oricăror alte activități ilegale sunt evidențiate, printre altele, la articolul 66 din Regulamentul privind Europol și la titlul X din Regulamentul financiar al Europol.

Europol participă, în special, la activitățile de prevenire a fraudei desfășurate de Oficiul European de Luptă Antifraudă (OLAF) și informează fără întârziere Comisia cu privire la cazurile de presupusă fraudă și de presupuse alte nereguli financiare – în conformitate cu strategia sa internă antifraudă.

În 2020, Consiliul de administrație a adoptat o actualizare a strategiei antifraudă a Europol.

Măsurile legate de combaterea fraudei, a corupției și a oricăror alte activități ilegale sunt evidențiate, printre altele, la articolul 50 din Regulamentul privind eu-LISA și la titlul X din Regulamentul financiar al eu-LISA.

Agenția eu-LISA participă, în special, la activitățile de prevenire a fraudei desfășurate de Oficiul European de Luptă Antifraudă (OLAF) și informează fără întârziere Comisia cu privire la cazurile de presupusă fraudă și de presupuse alte nereguli financiare – în conformitate cu strategia sa internă antifraudă.

În plus, în calitate de direcție generală parteneră, DG HOME a elaborat și a pus în aplicare o strategie antifraudă proprie pe baza metodologiei furnizate de OLAF. Agențiile descentralizate, inclusiv Europol și eu-LISA, intră în domeniul de aplicare al strategiei. Raportul anual de activitate pe 2020 al DG HOME a concluzionat că procesele de prevenire și detectare a fraudei au funcționat în mod satisfăcător și, prin urmare, au contribuit la asigurarea realizării obiectivelor de control intern.

(3) IMPACTUL FINANCIAR ESTIMAT AL INIȚIATIVEI LEGISLATIVE

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

Linii bugetare existente

În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul de cheltuieli	Contribuție			
	Numărul	Dif./Nedif. ⁴⁶	din partea țărilor AELS ⁴⁷	din partea țărilor candidate ⁴⁸	din partea țărilor terțe	în sensul articolului 21 alineatul (2) litera (b) din

⁴⁶ Dif. = credite diferențiate / Nedif. = credite nediferențiate.

⁴⁷ AELS: Asociația Europeană a Liberului Schimb.

⁴⁸ Țările candidate și, după caz, potențial candidate din Balcanii de Vest.

						Regulamentul financiar
--	--	--	--	--	--	------------------------

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul de cheltuieli	Contribuție			
	Numărul	Dif./Nedif.	din partea țărilor AELS	din partea țărilor candidate	din partea țărilor terțe	în sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar
5	12.02.01 – Fondul pentru securitate internă	Dif.	NU	NU	NU	NU
5	12.01.01 – Cheltuieli de sprijinire a Fondului pentru securitate internă	Nedif.	NU	NU	NU	NU
5	12.10.01 – Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol)	Nedif.	NU	NU	NU	NU
4	11.10.02 – Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA)	Nedif.	NU	NU	NU	NU

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual	5	Securitate și apărare
---	---	-----------------------

Europol			Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	TOTAL
Titlul 1: Cheltuieli cu personalul	Angajamente	(1)		0,551	1,102	0,847	0,847	3,347
	Plăți	(2)		0,551	1,102	0,847	0,847	3,347
Titlul 2: Cheltuieli de funcționare și cheltuieli cu infrastructura	Angajamente	(1a)		1,49	1,052	0,516	0,516	3,574
	Plăți	(2a)		1,49	1,052	0,516	0,516	3,574
Titlul 3: Cheltuieli operaționale	Angajamente	(3a)						
	Plăți	(3b)						
TOTAL credite pentru Europol	Angajamente	=1+1a +3a		2,041	2,154	1,363	1,363	6,921
	Plăți	=2+2a +3b		2,041	2,154	1,363	1,363	6,921

Observație: Creditele suplimentare solicitate în contextul prezentei propuneri pentru Europol vor fi acoperite din Fondul pentru securitate internă (FSI) de la rubrica 5.

Rubrica din cadrul financiar multianual	4	Migrație și frontiere
--	----------	------------------------------

eu-LISA			Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	TOTAL
Titlul 1: Cheltuieli cu personalul	Angajamente	(1)		0,456	0,988	1,52	1,45	4,414
	Plăți	(2)		0,456	0,988	1,52	1,45	4,414
Titlul 2: Cheltuieli de funcționare și cheltuieli cu infrastructura	Angajamente	(1a)		4,15	3,55	1,4	0	9,1
	Plăți	(2a)		4,15	3,55	1,4	0	9,1
Titlul 3: Cheltuieli operaționale	Angajamente	(3a)		0	0	1	1,2	2,2
	Plăți	(3b)		0	0	1	1,2	2,2
TOTAL credite pentru eu-LISA	Angajamente	=1+1a +3a		4,606	4,538	3,92	2,65	15,714
	Plăți	=2+2a +3b		4,606	4,538	3,92	2,65	15,714

Observație: Creditele suplimentare solicitate în contextul prezentei propuneri pentru eu-LISA vor fi acoperite din Instrumentul pentru gestionarea frontierelor și vize (IGFV) de la rubrica 4.

Rubrica din cadrul financiar multianual	5	Reziliență, securitate și apărare
--	----------	-----------------------------------

DG MIGRAȚIE ȘI AFACERI INTERNE (DG HOME)			Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	TOTAL
Fondul pentru securitate internă	Angajamente	(1)		13,64	40	40		93,64
	Plăți	(2)		4,68	6,55	9,39		34,65
TOTAL credite pentru DG HOME	Angajamente			13,64	40	40		93,64
	Plăți			4,68	6,55	9,39		34,65

Observație: Creditele solicitate în contextul prezentei propuneri vor fi acoperite de credite deja prevăzute în fișa financiară legislativă care stă la baza Regulamentului privind FSI. Nu sunt necesare resurse financiare sau umane suplimentare în contextul prezentei propuneri legislative.

Costurile pentru fiecare stat membru includ:

- modernizarea infrastructurii lor pentru a sprijini schimbul de servicii web și stabilirea conexiunii cu routerul central, ceea ce implică eforturi de analiză și definire a noii arhitecturi;
- modernizarea infrastructurii lor pentru a sprijini schimbul de servicii web și stabilirea conexiunii cu routerul central;
- configurarea unui sistem de schimb de servicii web și configurarea conexiunii cu routerul central;
- proiectarea unei noi arhitecturi naționale și a specificațiilor pentru a asigura accesul la datele naționale prin intermediul soluțiilor dezvoltate (router și EPRIS);
- crearea unui nou registru sau punerea la dispoziție a unui registru deja existent pentru schimbul de cazieri judiciare;

- crearea unei noi baze de date cu imagini faciale sau punerea la dispoziție pentru schimb a unei baze de date cu imagini faciale deja existente;
- integrarea soluției naționale;
- costurile generice legate de gestionarea proiectului.

Tabelul următor indică costurile pe categorii:

A se indica obiectivele și realizările DG Migrație și Afaceri Interne (DG HOME) ↓			Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	TOTAL					
	Tipul	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Total nr.	Total costuri
Routerul	Conectarea la router a bazelor de date existente			26	2,314	26	6,787	26	6,787			26	15,89
Imagini faciale	Crearea unei noi baze de date			13*	2,84	13	8,329	13	8,329			13	19,5
	Conectarea bazei de date la router			26	2,72	26	7,996	26	7,996			26	18,72
Caziere judiciare	Crearea unei baze de date a cazierelor judiciare și conectarea la EPRIS			26	5,763	26	16,959	26	16,959			26	39,7

Total			13,64		40		40			93,64
-------	--	--	-------	--	----	--	----	--	--	-------

*Estimare SM fără o bază de date cu imagini faciale

Rubrica din cadrul financiar multianual	7	Cheltuieli administrative
--	----------	---------------------------

milioane EUR (cu trei zecimale)

		Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	TOTAL	
DG: HOME								
• Resurse umane			0,608	0,684	0,608	0,608	2,508	
• Alte cheltuieli administrative			0,225	0,225	0,186	0,186	0,822	
TOTAL pentru DG HOME	Credite							

TOTAL credite de la RUBRICA 7 din cadrul financiar multianual	(Total angajamente = Total plăți)		0,833	0,833	0,794	0,794	3,330	
--	-----------------------------------	--	-------	-------	-------	-------	-------	--

milioane EUR (cu trei zecimale)

		Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	TOTAL
TOTAL credite de la RUBRICILE 1-5 din cadrul financiar multianual	Angajamente		20,287	46,692	45,283	4,013	116,275
	Plăți		11,329	13,247	14,647	18,059	57,282

3.2.2. Impactul estimat asupra creditelor Europol

- ☐ Propunerea/inițiativa nu implică utilizarea de credite operaționale.
- ☒ Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos:

Credite de angajament în milioane EUR (cu trei zecimale)

A se indica obiectivele și realizările			Anul		Anul		Anul		Anul		Anul		TOTAL	
			2023		2024		2025		2026		2027			
↓	Tipul	Costuri medii ⁴⁹	Numărul	Costuri	Numărul	Costuri	Numărul	Costuri	Numărul	Costuri	Numărul	Costuri	Numărul	Costuri
Costurile Europol (care nu sunt legate de resursele umane)														
– Realizare	Infrastructură și întreținere					0,764		0,326		0,226		0,226		1,542
– Realizare	Contractanți					0,726		0,726		0,290		0,290		2,032
COSTURI TOTALE						1,490		1,052		0,516		0,516		3,574

⁴⁹ Având în vedere natura operațională specifică a acestora, nu este posibilă identificarea unor costuri unitare precise pentru fiecare realizare și nici a unui volum exact preconizat al realizărilor, în special deoarece unele realizări vizează activități de asigurare a respectării legii care trebuie să se adapteze la activități infracționale imprevizibile.

3.2.3. Impactul estimat asupra creditelor eu-LISA

- ☐ Propunerea/inițiativa nu implică utilizarea de credite operaționale.
- ☒ Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos:

Credite de angajament în milioane EUR (cu trei zecimale)

A se indica obiectivele și realizările			Anul		Anul		Anul		Anul		Anul		TOTAL	
			2023		2024		2025		2026		2027			
↓	Tipul	Costuri medii ⁵⁰	Numărul	Costuri	Numărul	Costuri	Numărul	Costuri	Numărul	Costuri	Numărul	Costuri	Numărul	Costuri
Costurile eu-LISA (care nu sunt legate de resursele umane)														
– Realizare	Infrastructură ⁵¹					1,85		2,15		0,7		0		4,7

⁵⁰ Având în vedere natura operațională specifică a acestora, nu este posibilă identificarea unor costuri unitare precise pentru fiecare realizare și nici a unui volum exact preconizat al realizărilor, în special deoarece unele realizări vizează activități de asigurare a respectării legii care trebuie să se adapteze la activități infracționale imprevizibile.

⁵¹ Sunt incluse costurile cu hardware, software, furnizarea de rețele, securitatea.

– Realizare	Contractanți ⁵²					1,4		0,7		0,7		0		2,8
– Realizare	Mecanism de stabilire a unei microconcordanțe					0,9		0,7		0		0		
– Realizare	Întreținere					0		0		1		1,2		2,2
COSTURI TOTALE						4,15		3,55		2,4		1,2		11,3

⁵² Sunt incluse costurile cu serviciile profesionale, proiectarea și testarea.

3.2.4. Impactul estimat asupra resurselor umane ale Europol

3.2.4.1. Rezumat

☐ Propunerea/inițiativa nu implică utilizarea de credite cu caracter administrativ.

☒ Propunerea/inițiativa implică utilizarea de credite cu caracter administrativ, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

	Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	TOTAL
--	--------------	--------------	--------------	--------------	--------------	-------

Angajați temporari – nivel de referință						
Angajați temporari – în plus față de nivelul de referință (cumulativ)	0	0,551	1,101	0,847	0,847	3,347
Angajați temporari – TOTAL						
Personal contractual – nivel de referință						
Experți naționali detașați – nivel de referință (solicitare în proiectul de buget pe 2021)						

TOTAL – Numai costurile suplimentare	0	0,551	1,101	0,847	0,847	3,347
TOTAL – Inclusiv costurile de referință și costurile suplimentare						

Cerințe privind personalul (ENI):

	Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027
Angajați temporari – nivel de referință	0	9,5	9,5	21,5	19,5
Angajați temporari – în plus față de nivelul de referință (cumulativ)	0	6,5	6,5	5	5
Angajați temporari – TOTAL		16	16	26,5	24,5
Personal contractual					

Experți naționali detașați					
TOTAL	0	16,5	16,5	26,5	24,5

Resursele umane necesare pentru punerea în aplicare a obiectivelor prezentei propuneri au fost estimate în cooperare cu Europol. Estimările iau în considerare creșterea preconizată a volumului de muncă pe măsură ce părțile interesate vor recurge tot mai mult la serviciile Europol, precum și timpul de care va avea nevoie Europol pentru a absorbi resursele, în vederea evitării unei situații în care agenția nu ar putea să execute integral contribuția UE și să angajeze creditele în timp util.

Resursele umane necesare pentru punerea în aplicare a obiectivelor prezentei propuneri vor fi acoperite parțial de personalul existent în cadrul Europol (nivelul de referință) și parțial de resurse suplimentare (personal suplimentar față de scenariul de referință).

Fișa financiară legislativă nu prevede o creștere a numărului de angajați contractuali.

Pentru punerea în aplicare a Prüm II, resursele necesare pentru Europol pot fi împărțite în 3 categorii:

- 1) costuri TIC pentru conectarea la routerul biometric din cadrul eu-LISA, lucrări de dezvoltare necesare în sistemele de informații ale Europol pentru a face disponibile datele provenite de la terți pentru căutări efectuate de statele membre și pentru a integra căutările în Prüm cu datele provenite de la terți în interfața unică de căutare a Europol USE-UI;
- 2) costuri cu personalul din cadrul Direcției Operațiuni a Europol care va efectua căutări în datele provenite de la terți și costuri cu experții în materie de date biometrice care vor efectua verificarea rezultatelor pozitive;
- 3) găzduirea unui router central pentru cazierile judiciare. Aceasta va include costuri unice pentru hardware (inclusiv medii diferite de producție și testare pentru statele membre), personal TIC care să asigure dezvoltarea și gestionarea modificărilor software-ului ADEP.EPRIS, testarea împreună cu statele membre, serviciu de asistență 24/7 pentru a sprijini statele membre în cazul în care întâmpină probleme. Pentru a asigura un sprijin deplin statelor membre, este nevoie de disponibilitatea unor profiluri diferite de personal TIC, de exemplu coordonare generală, ingineri responsabili cu cerințele, dezvoltatori, testatori, administratori de sistem. Se preconizează că va fi încă nevoie de un număr puțin mai mare de membri ai personalului TIC în primul an după punerea în funcțiune.

Din cauza constrângerilor de securitate și a plafonului convenit pentru agenții contractuali, majoritatea sarcinilor legate de Prüm trebuie îndeplinite de personalul Europol. Se preconizează externalizarea anumitor activități mai puțin sensibile către contractanți (testare, unele sarcini de dezvoltare).

Agenți temporari în ENI (nivel de referință + personal suplimentar)	2023	2024	2025	2026	2027
Managementul proiectelor		1,0	1,0	0,5	0,5

Experți (total)		14,5	14,5	18,0	16,0
• <i>date biometrice</i>		1,0	1,0	4,0	4,0
• <i>personal operativ</i>		0,5	0,5	4,0	4,0
• <i>TIC</i>		13,0	13,0	10,0	8,0
Asistență/monitorizare la nivelul serviciului de asistență		0,0	0,0	7,0	7,0
Coordonare generală		1,0	1,0	1,0	1,0
Total		16,5	16,5	26,5	24,5

3.2.5. Impactul estimat asupra resurselor umane ale eu-LISA

3.2.5.1. Rezumat

- ☐ Propunerea/inițiativa nu implică utilizarea de credite cu caracter administrativ.
- ☒ Propunerea/inițiativa implică utilizarea de credite cu caracter administrativ, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

	Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	TOTAL
--	--------------	--------------	--------------	--------------	--------------	-------

Angajați temporari – nivel de referință						
Angajați temporari – în plus față de nivelul de referință (cumulativ)		0,456	0,988	1,52	1,368	4,332
Angajați temporari – TOTAL						
Personal contractual – nivel de referință						
Personal contractual – suplimentar					0,082	0,082
Experți naționali detașați – nivel de referință (solicitare în proiectul de buget pe 2021) ⁵³						

TOTAL – Numai costurile suplimentare		0,456	0,988	1,52	1,45	4,414
TOTAL – Inclusiv costurile de referință și costurile suplimentare						

⁵³ Nivelurile de personal indicate în proiectul de buget pe 2021, calculate pe baza costurilor unitare medii cu personalul care trebuie utilizate pentru fișa financiară legislativă. Se calculează o jumătate din creditele anuale corespunzătoare pentru anul în care este recrutat personalul.

Cerințe privind personalul (ENI):

	Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027
Angajați temporari – nivel de referință					
Angajați temporari – în plus față de nivelul de referință (cumulativ)		6	7	10	9
Angajați temporari – TOTAL					
Personal contractual – nivel de referință					
Personal contractual – suplimentar					2
Experți naționali detașați					
TOTAL		6	7	10	11

Resursele umane necesare pentru punerea în aplicare a obiectivelor noului mandat au fost estimate în cooperare cu eu-LISA. Estimările iau în considerare creșterea preconizată a volumului de muncă pe măsură ce părțile interesate vor recurge tot mai mult la serviciile eu-LISA, precum și timpul de care va avea nevoie eu-LISA pentru a absorbi resursele, în vederea evitării unei situații în care agenția nu ar putea să execute integral contribuția UE și să angajeze creditele în timp util.

Aceste estimări se bazează pe următoarea schemă de personal:

	Etapă								
	Analiză și proiectare			Construire și dezvoltare			Funcționare		
Tipul de contract	AT	AC	Total	AT	AC	Total	AT	AC	Total
Profil	Nr.	Nr.		Nr.	Nr.		Nr.	Nr.	
Arhitect IT	1		1	1		1	1		1
Managementul testelor	1		1	1		1	0,5		0,5
Gestionarea versiunilor și a modificărilor			0	1		1	1		1
Administrator de rețea	1		1	1		1	1		1
Managementul securității	2		2	2		2	2		2
Operator asistență nivel 1 (24/7)			0			0		1	1
Operator asistență			0			0		1	1

nivel 2 (24/7)									
Managementul programelor și proiectelor	1		1	1		1	0,5		0,5
Proprietarul produsului			0	1		1	1		1
Expert date biometrice	1		1	1		1	1		1
Administrator de sistem/Infrastructură	1		1	1		1	1		1
Total (AC+AT)	8		8	10		10	9	2	11

Profiluri	Anul -1 (Pregătire și proiectare)	Anul 1	Anul 2	Anul 3	Anul 4	Anul 5
Arhitect IT (AT)	1	1	1	1	1	1
Managementul testelor (AT)		1	1	0,5	0,5	0,5
Gestionarea versiunilor și a modificărilor (AT)			1	1	1	1
Administrator de rețea	1	1	1	1	1	1

(AT)						
Managementul securității (AT)	1	1	2	2	2	2
Operator asistență nivel 1 (24/7) – (AC)				1	1	1
Operator asistență nivel 2 (24/7) – (AC)				1	1	1
Managementul programelor și proiectelor (AT)	1	1	1	0,5	0,5	0,5
Proprietarul produsului (AT)			1	1	1	1
Expert date biometrice (AT)	1	1	1	1	1	1
Administrator de sistem/ Infrastructură (AT)	1	1	1	1	1	1
TOTAL	6	7	10	11	11	11

3.2.5.2. Necesarul de resurse umane estimat pentru direcția generală parteneră

☐ Propunerea/inițiativa nu implică utilizarea de resurse umane.

☒ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

Estimarea se exprimă în numere întregi (sau cel mult cu o zecimală)

	Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027
• Posturi din schema de personal (funcționari și agenți temporari)					
XX 01 01 01 (la sediu și în reprezentanțele Comisiei)		5	5	4	4
XX 01 01 02 (în delegații)					
XX 01 05 01 (cercetare indirectă)					
10 01 05 01 (cercetare directă)					
• Personal extern (în echivalent normă întreagă: ENI)⁵⁴					
XX 01 02 01 (AC, END, INT din „pachetul global”)					
XX 01 02 02 (AC, AL, END, INT și JPD în delegații)					
XX 01 04 yy ⁵⁵	– la sediu ⁵⁶				
	– în delegații				
XX 01 05 02 (AC, END, INT – cercetare indirectă)					
10 01 05 02 (AC, INT, END – cercetare directă)					
Alte linii bugetare (a se preciza)					
TOTAL		5	5	4	4

XX este domeniul de politică sau titlul bugetar în cauză.

Necesarul de resurse umane va fi asigurat parțial (3 ENI) din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând seama de constrângerile bugetare. Direcția generală va avea nevoie, de asemenea, de personal suplimentar (2 ENI).

⁵⁴ AC = agent contractual; AL = agent local; END = expert național detașat; INT = personal pus la dispoziție de agenți de muncă temporară; JPD = expert tânăr în delegații.

⁵⁵ Subplafonul pentru personal extern acoperit din creditele operaționale (fostele linii „BA”).

⁵⁶ În principal pentru fondurile structurale, Fondul european agricol pentru dezvoltare rurală (FEADR) și Fondul european pentru pescuit (FEP).

Descrierea sarcinilor care trebuie efectuate:

Cinci funcționari pentru acțiuni ulterioare. Personalul care se ocupă de preluarea atribuțiilor Comisiei în ceea ce privește livrarea programului: verificarea conformității cu propunerea legislativă, abordarea aspectelor legate de conformitate, elaborarea de rapoarte adresate Parlamentului European și Consiliului, evaluarea progreselor înregistrate de statele membre, actualizarea legislației secundare, inclusiv orice evoluție referitoare la standarde. Întrucât acest program reprezintă o activitate suplimentară față de volumul de lucru existent, este nevoie de personal suplimentar (2 ENI). Una dintre creșterile de personal este limitată în ceea ce privește durata și acoperă doar perioada de dezvoltare, iar cea de-a doua reprezintă absorbția atribuțiilor Secretariatului Consiliului – întrucât deciziile Consiliului sunt transformate într-un regulament, Comisia trebuie să preia atribuțiile Secretariatului Consiliului cu 1 ENI.

3.2.6. Compatibilitatea cu cadrul financiar multianual actual

- ☐ Propunerea/inițiativa este compatibilă cu actualul cadru financiar multianual.
- ☐ Propunerea/inițiativa necesită o reprogramare a rubricii corespunzătoare din cadrul financiar multianual.

- ☐ Propunerea/inițiativa necesită recurgerea la instrumentul de flexibilitate sau revizuirea cadrului financiar multianual⁵⁷.

A se explica necesitatea efectuării acestei acțiuni, precizând rubricile și liniile bugetare vizate, precum și sumele aferente.

[...]

3.2.7. Contribuțiile terților

Propunerea/inițiativa nu prevede cofinanțare din partea terților.

Propunerea/inițiativa prevede cofinanțarea estimată în cele ce urmează:

milioane EUR (cu trei zecimale)

	Anul N	Anul N+1	Anul N+2	Anul N+3	Se vor introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)			Total
A se preciza organismul care asigură cofinanțarea								
TOTAL credite cofinanțate								

⁵⁷ A se vedea articolele 11 și 17 din Regulamentul (UE, Euratom) nr. 1311/2013 al Consiliului de stabilire a cadrului financiar multianual pentru perioada 2014-2020.

3.3. Impactul estimat asupra veniturilor

- ☒ Propunerea/inițiativa nu are impact financiar asupra veniturilor.
- ☐ Propunerea/inițiativa are următorul impact financiar:
- ☐ asupra resurselor proprii
 - ☐ asupra altor venituri
 - ☐ vă rugăm să precizați dacă veniturile sunt alocate unor linii de cheltuieli

milioane EUR (cu trei zecimale)

Linia bugetară pentru venituri:	Credite disponibile pentru exercițiul financiar în curs	Impactul propunerii/inițiativei ⁵⁸						
		Anul N	Anul N+1	Anul N+2	Anul N+3	Se vor introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)		
Articolul								

Pentru diversele venituri alocate, a se preciza linia bugetară (liniile bugetare) de cheltuieli afectată (afectate).

[...]

A se preciza metoda de calcul al impactului asupra veniturilor.

[...]

⁵⁸ În ceea ce privește resursele proprii tradiționale (taxe vamale, cotizații pentru zahăr), sumele indicate trebuie să fie sume nete, și anume sumele brute după deducerea unei cote de 20 % pentru costurile de colectare.

ANEXA 5

la

DECIZIA COMISIEI

**referitoare la normele interne privind execuția bugetului general al Uniunii Europene (secțiunea
Comisia Europeană) în atenția departamentelor Comisiei**

ANEXĂ

la FIȘA FINANCIARĂ LEGISLATIVĂ

ANEXĂ **la FIȘA FINANCIARĂ LEGISLATIVĂ**

Titlul propunerii:

Propunere privind schimbul automatizat de date în scopul cooperării polițienești („Prüm II”), de modificare a Regulamentelor (UE) 2018/1726, 2019/817 și 2019/818 și de abrogare a Deciziilor 2008/615/JAI și 2008/616/JAI ale Consiliului

- 1. NUMĂRUL ȘI COSTURILE AFERENTE RESURSELOR UMANE CONSIDERATE NECESARE**
- 2. COSTURI AFERENTE ALTOR CHELTUIELI ADMINISTRATIVE**
- 3. TOTAL CHELTUIELI ADMINISTRATIVE**
- 4. METODE DE CALCUL UTILIZATE PENTRU ESTIMAREA COSTURILOR**
 - 4.1. Resurse umane**
 - 4.2. Alte cheltuieli administrative**

Prezenta anexă trebuie să însoțească fișa financiară legislativă atunci când se lansează consultarea interservicii.

Tabelele de date sunt utilizate ca sursă pentru tabelele conținute în fișa financiară legislativă. Acestea sunt destinate exclusiv uzului intern în cadrul Comisiei.

(1) Costurile aferente resurselor umane considerate necesare

☐ Propunerea/inițiativa nu implică utilizarea de resurse umane.

☒ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

RUBRICA 7 din cadrul financiar multianual		2024		2025		2026		2027								TOTAL	
		ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite
• Posturi din schema de personal (funcționari și agenți temporari)																	
20 01 02 01 – Sediul central și reprezentanțele	AD	5	0,608	5	0,684	4	0,608	4	0,608							4	2,508
	AST																
20 01 02 03 - Delegațiile Uniunii	AD																
	AST																
• Personal extern ⁵⁹																	
20 02 01 și 20 02 02 – Personal extern – Sediul central și reprezentanțe	AC																
	END																
	INT																
20 02 03 – Personal extern - Delegațiile Uniunii	AC																
	AL																
	END																

⁵⁹ AC = agent contractual; AL = agent local; END = expert național detașat; INT = personal pus la dispoziție de agenți de muncă temporară; JPD = expert tânăr în delegații.

	INT																
	JPD																
Alte linii bugetare legate de resursele umane (a se preciza)																	
Subtotal RU – RUBRICA 7		5	0,608	5	0,684	4	0,608	4	0,608							4	2,508

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând seama de constrângerile bugetare.

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând seama de constrângerile bugetare.

(2) Costuri aferente altor cheltuieli administrative

☐ Propunerea/inițiativa nu implică utilizarea de credite administrative.

☒ Propunerea/inițiativa implică utilizarea de credite administrative, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

RUBRICA 7 din cadrul financiar multianual	2024	2025	2026	2027				Total
La sediu sau pe teritoriul UE:								
20 02 06 01 – Cheltuieli pentru efectuarea de delegații și cheltuieli de reprezentare	0,035	0,035	0,035	0,035				0,140
20 02 06 02 – Costuri aferente conferințelor și reuniunilor	0,125	0,125	0,125	0,125				0,500
20 02 06 03 – Comitete (Comitetul Prüm II) ⁶⁰	0,065	0,065	0,026	0,026				0,182
20 02 06 04 – Studii și consultări								
20 04 – Cheltuieli IT (corporative) ⁶¹								
Alte linii bugetare care nu sunt legate de resursele umane (a se preciza dacă este necesar)								
În delegațiile Uniunii								
20 02 07 01 – Cheltuieli pentru delegații, conferințe și reprezentare								

⁶⁰ Comitetul Prüm II, aproximativ 10 reuniuni pe an în 2024 și 2025 și 4 reuniuni pe an ulterior, doar jumătate dintre acestea fiind contabilizate în cadrul costurilor (cealaltă jumătate - în format de videoconferință).

⁶¹ Este necesar avizul DG DIGIT – Echipa de investiții IT [a se vedea Orientările privind finanțarea IT, C(2020) 6126 final din 10.9.2020, pagina 7].

20 02 07 02 – Activități de perfecționare a personalului								
20 03 05 – Infrastructură și logistică								
Alte linii bugetare care nu sunt legate de resursele umane (a se preciza dacă este necesar)								
Subtotal altele – RUBRICA 7 din cadrul financiar multianual	0,225	0,225	0,186	0,186				0,822

milioane EUR (cu trei zecimale)

În afara RUBRICII 7 din cadrul financiar multianual	2024	2025	2026	2027				Total
Cheltuieli cu asistența tehnică și administrativă (cu excepția personalului extern) din creditele operaționale (fostele linii „BA”):								
– la sediu								
– în delegațiile Uniunii								
Alte cheltuieli de gestiune pentru cercetare								
Politica de cheltuieli IT privind programele operaționale ⁶²								
Cheltuieli IT corporative pentru programele								

⁶²

Este necesar avizul DG DIGIT – Echipa de investiții IT [a se vedea Orientările privind finanțarea IT, C(2020) 6126 final din 10.9.2020, pagina 7].

operaționale ⁶³								
Alte linii bugetare care nu sunt legate de resursele umane (a se preciza dacă este necesar)								
Subtotal altele – în afara RUBRICII 7 din cadrul financiar multianual								
Total alte cheltuieli administrative (toate rubricile CFM)	0,225	0,225	0,186	0,186				0,822

⁶³ Acest element include sistemele administrative locale și contribuțiile la cofinanțarea sistemelor informatice corporative [a se vedea Orientările privind finanțarea IT, C(2020) 6126 final din 10.9.2020].

(3) Total costuri administrative (toate rubricile CFM)

milioane EUR (cu trei zecimale)

Rezumat	2024	2025	2026	2027				Total
Rubrica 7 – Resurse umane	0,608	0,684	0,608	0,608				2,508
Rubrica 7 – Alte cheltuieli administrative	0,225	0,225	0,186	0,186				0,822
Subtotal Rubrica 7								
În afara Rubricii 7 – Resurse umane								
În afara Rubricii 7 – Alte cheltuieli administrative								
Subtotal alte rubrici								
TOTAL RUBRICA 7 și în afara RUBRICII 7	0,833	0,833	0,794	0,794				3,330

Necesarul de credite administrative va fi asigurat din creditele alocate deja pentru gestionarea acțiunii și/sau realocate, completate, după caz, prin resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii de alocare anuală și în lumina constrângerilor bugetare existente.

4. METODELE DE CALCULARE UTILIZATE PENTRU ESTIMAREA COSTURILOR

4.1. Resurse umane

Această parte stabilește metoda de calculare utilizată pentru estimarea resurselor umane considerate necesare [ipoteze referitoare la volumul de muncă, inclusiv posturi specifice (profiluri profesionale specifice sistemului Sysper2), categoriile de personal și costurile medii aferente]

RUBRICA 7 din cadrul financiar multianual

NB: Costurile medii pentru fiecare categorie de personal de la sediul central sunt disponibile pe BudgWeb:
https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx

Funcționari și personal temporar:

În conformitate cu circulara DG BUGET la RUF/2020/23 din 30.11.2020 [a se vedea anexa 1, Ares (2020) 7207955 din 30.11.2020], 1 AD reprezintă un cost de 152 000 EUR pe an. Jumătate din creditul anual corespunzător se calculează pentru anul în care personalul este recrutat și redus treptat.

Necesarul de resurse umane va fi asigurat parțial (3 ENI) din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând seama de constrângerile bugetare. Direcția generală va avea nevoie, de asemenea, de personal suplimentar (2 ENI).

Descrierea sarcinilor care trebuie efectuate:

Cinci funcționari pentru acțiuni ulterioare. Personalul care se ocupă de preluarea atribuțiilor Comisiei în ceea ce privește livrarea programului: verificarea conformității cu propunerea legislativă, abordarea aspectelor legate de conformitate, elaborarea de rapoarte adresate Parlamentului European și Consiliului, evaluarea progreselor înregistrate de statele membre, actualizarea legislației secundare, inclusiv orice evoluție referitoare la standarde. Întrucât acest program reprezintă o activitate suplimentară față de volumul de lucru existent, este nevoie de personal suplimentar (2 ENI). Una dintre creșterile de personal este limitată în ceea ce privește durata și acoperă doar perioada de dezvoltare, iar cea de-a doua reprezintă absorbția atribuțiilor Secretariatului Consiliului – întrucât deciziile Consiliului sunt transformate într-un regulament, Comisia trebuie să preia atribuțiile Secretariatului Consiliului cu 1 ENI.

- Personal extern

În afara RUBRICII 7 din cadrul financiar multianual

- Numai posturile finanțate din bugetul de cercetare

- Personal extern

4.2. Alte cheltuieli administrative

*A se detalia metoda de calcul utilizată pentru fiecare linie bugetară
și în special ipotezele pe care se bazează (de exemplu, numărul de reuniuni pe an, costurile medii etc.)*

RUBRICA 7 din cadrul financiar multianual

Se estimează că, în medie, vor avea loc 35 de delegații pe an, inclusiv delegațiile pentru reuniunile statutare (Grupul consultativ, grupurile de lucru ale eu-LISA și ale Europol și reuniunile legate de EPRIS și Eucaris), pentru a participa la reuniunile și conferințele legate de cadrul Prüm. Costul unitar per delegație se calculează presupunând că 1 funcționar se deplasează pentru 2 zile în medie pentru fiecare delegație și este stabilit la 500 EUR per delegație pe zi.

Costurile unitare per reuniune/conferință de experți sunt stabilite la 25 000 EUR pentru 50 de participanți. Se estimează că vor fi organizate 5 reuniuni pe an.

Costurile unitare per comitet sunt stabilite la 13 000 EUR pentru 26 de participanți, presupunând rambursarea pentru 1 participant per stat membru pentru o delegație de o zi la comitet. Se estimează că vor fi organizate 10 reuniuni pe an în 2024 și 2025 (5 în format fizic și 5 în format de videoconferință) și 4 reuniuni pe an începând din 2026 (2 în format fizic și 2 în format de videoconferință).

În afara RUBRICII 7 din cadrul financiar multianual