Consiliul
Uniunii Europene

Bruxelles, 19 ianuarie 2018
(OR. en)

15119/17
COR 1

Dosar interinstituțional:
2017/0351 (COD)

COSI 336 **FAUXDOC 73**
FRONT 507 **COPEN 419**
ASIM 142 **JAI 1212**
DAPIX 430 **CT 164**
ENFOPOL 622 **CSCI 79**
ENFOCUSTOM 285 **SAP 28**
SIRIS 217 **COMIX 840**
SCHENGEN 88 **CODEC 2153**
DATAPROTECT 220 **IA 232**
VISA 458

PROPUNERE

Sursă:	Secretar general al Comisiei Europene, sub semnătura dlui Jordi AYET PUIGARNAU, director
Data primirii:	14 decembrie 2017
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2017) 793 final
Subiect:	Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE (în materie de frontiere și vize) și de modificare a Deciziei 2004/512/CE a Consiliului, a Regulamentului (CE) nr. 767/2008, a Deciziei 2008/633/JAI a Consiliului, a Regulamentului (UE) 2016/399 și a Regulamentului (UE) 2017/2226

Codurile de domeniu ale documentului ST 15119/17 INIT se citesc după cum urmează:

COSI 336
FRONT 507
ASIM 142
DAPIX 430
ENFOPOL 622
ENFOCUSTOM 285
SIRIS 217
SCHENGEN 88
DATAPROTECT 220
VISA 458
FAUXDOC 73
COPEN 419

COMISIA
EUROPEANĂ

Strasbourg, 12.12.2017
COM(2017) 793 final

2017/0351 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE (în materie de frontiere și vize) și de modificare a Deciziei 2004/512/CE a Consiliului, a Regulamentului (CE) nr. 767/2008, a Deciziei 2008/633/JAI a Consiliului, a Regulamentului (UE) 2016/399 și a Regulamentului (UE) 2017/2226

{SWD(2017) 473 final} - {SWD(2017) 474 final}

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

• Contextul propunerii

În ultimii trei ani, UE s-a confruntat cu o creștere a numărului de cazuri de trecere neregulamentară a frontierelor UE și cu o amenințare crescândă și continuă la adresa securității interne, fapt demonstrat de o serie de atacuri teroriste. Cetățenii UE se așteaptă ca atât controlul persoanelor la frontierele externe, cât și verificările în spațiul Schengen să fie eficace, să permită gestionarea eficace a migrației și să contribuie la securitatea internă. Aceste provocări au readus în prim-plan necesitatea de a reuni și de a consolida de urgență și într-o manieră cuprinzătoare instrumentele de informații de care dispune UE în domeniul gestionării frontierelor, al migrației și al securității.

Este nevoie de o gestionare mai eficace și mai eficientă a informațiilor în UE, cu respectarea deplină a drepturilor fundamentale, în special a dreptului la protecția datelor cu caracter personal, pentru a asigura o mai bună protecție a frontierelor externe ale UE, îmbunătățirea gestionării migrației și consolidarea securității interne, în beneficiul tuturor cetățenilor. La nivelul UE, există deja o serie de sisteme de informații, iar altele sunt în curs de instituire; cu ajutorul acestor sisteme, polițiștii de frontieră, funcționarii din cadrul serviciilor de imigrație și agenții responsabili cu aplicarea legii au acces la informații relevante asupra persoanelor. Pentru ca acest sprijin să fie eficace, informațiile furnizate de sistemele de informații ale UE trebuie să fie complete, exacte și fiabile. Există însă probleme structurale în arhitectura UE de gestionare a informațiilor. Autoritățile naționale se confruntă cu un peisaj complex, alcătuit din sisteme de informații reglementate în mod diferit. În plus, arhitectura de gestionare a datelor privind frontierele și securitatea este fragmentată, întrucât informațiile sunt stocate separat în sisteme care nu sunt interconectate. Din acest motiv apar așa-numitele „unghiuri moarte”. În consecință, **diferitele sisteme de informații existente la nivelul UE nu sunt interoperabile**, adică nu permit schimbul de date și de informații, astfel încât autoritățile și funcționarii competenți să aibă acces la informațiile de care au nevoie, la momentul și locul oportun. Interoperabilitatea sistemelor de informații de la nivelul UE poate contribui în mod semnificativ la eliminarea unghiurilor moarte actuale – respectiv situațiile în care anumite persoane, inclusiv persoane care ar putea fi implicate în activități teroriste, sunt înregistrate sub pseudonime diferite în baze de date diferite care nu sunt interconectate.

În aprilie 2016, Comisia a prezentat o **comunicare intitulată *„Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”***[1] pentru a soluționa o serie de deficiențe structurale legate de sistemele de informații[2]. Scopul comunicării din aprilie 2016 a fost inițierea unei discuții cu privire la modul în care sistemele de informații din Uniunea Europeană pot consolida în continuare gestionarea frontierelor și a migrației și securitatea internă. **Consiliul** a recunoscut, la rândul său, că se impune adoptarea urgentă a unor măsuri în acest domeniu. În iunie 2016, Consiliul a adoptat o **foaie de parcurs pentru a consolida schimbul de informații și gestionarea informațiilor**, inclusiv soluțiile de interoperabilitate, în domeniul justiției și afacerilor interne[3]. Obiectivul foii de parcurs era acela de a sprijini investigațiile operaționale și de a pune

[1] COM(2016) 205 din 6 aprilie 2016.

[2] (1) funcționalități sub nivelul optim pentru o parte dintre sistemele de informații existente; (2) lacune în materie de informații în arhitectura UE de gestionare a datelor; (3) un peisaj complex, alcătuit din sisteme de informații reglementate în mod diferit și (4) o arhitectură fragmentată de gestionare a datelor în materie de frontiere și securitate, în care informațiile sunt stocate separat în sisteme care nu sunt interconectate, ceea ce conduce la apariția unor unghiuri moarte.

[3] Foaia de parcurs din 6 iunie 2016 pentru a consolida schimbul de informații și gestionarea informațiilor, inclusiv soluțiile de interoperabilitate, în domeniul justiției și afacerilor interne – 9368/1/16 REV 1.

rapid la dispoziția practicienilor din prima linie, cum ar fi agenții de poliție, polițiștii de frontieră, procurorii, funcționarii din cadrul serviciilor de imigrație, informații cuprinzătoare, de actualitate și de înaltă calitate, care să le permită să coopereze și să acționeze în mod eficace. La rândul său, **Parlamentul European** a solicitat adoptarea de măsuri în acest domeniu. În Rezoluția sa din iulie 2016[4] privind programul de lucru al Comisiei pentru 2017, Parlamentul European a solicitat Comisiei să își prezinte „*propunerile pentru îmbunătățirea și dezvoltarea sistemelor de informații existente, abordarea lacunelor în materie de informații și tranziția către interoperabilitate, precum și propunerile privind obligativitatea schimbului de informații la nivelul UE, însoțite de garanțiile necesare în materie de protecție a datelor*”. Discursul privind starea Uniunii pronunțat de președintele Juncker în septembrie 2016[5] și concluziile Consiliului European din decembrie 2016[6] au evidențiat importanța depășirii deficiențelor actuale în domeniul gestionării datelor și a adoptării de măsuri pentru îmbunătățirea interoperabilității sistemelor de informații existente.

În iunie 2016, ca urmare a comunicării din aprilie 2016, Comisia a înființat **un grup de experți la nivel înalt pentru sistemele de informații și interoperabilitate**[7] pentru a aborda provocările juridice, tehnice și operaționale legate de consolidarea interoperabilității între sistemele centrale ale UE în materie de frontiere și securitate, inclusiv pentru a aborda chestiunea necesității, a fezabilității tehnice, a proporționalității și a implicațiilor asupra protecției datelor ale unei astfel de consolidări. **Raportul final** întocmit de grupul de experți la nivel înalt a fost publicat în mai 2017[8]. Acest raport cuprinde o serie de recomandări menite să consolideze și să dezvolte sistemele de informații ale UE și interoperabilitatea acestora. La lucrările grupului de experți au participat activ Agenția pentru Drepturi Fundamentale a Uniunii Europene, Autoritatea Europeană pentru Protecția Datelor și coordonatorul UE pentru lupta împotriva terorismului. Toate aceste instituții și-au exprimat susținerea față de această inițiativă, recunoscând însă faptul că, pentru a face progrese în această direcție, trebuie abordate aspecte mai largi privind drepturile fundamentale și protecția datelor. Reprezentanți ai Secretariatului Comisiei pentru libertăți civile, justiție și afaceri interne a Parlamentului European și ai Secretariatului General al Consiliului au participat în calitate de observatori. Grupul de experți la nivel înalt a concluzionat că este **necesar și posibil din punct de vedere tehnic să se găsească soluții practice pentru realizarea interoperabilității** și că acestea pot, în principiu, să ofere câștiguri operaționale, și, totodată, să fie instituite în conformitate cu cerințele în materie de protecție a datelor.

Pe baza raportului și a recomandărilor grupului de experți, Comisia a prezentat, în cel de *Al șaptelea raport privind progresele înregistrate pentru realizarea unei uniuni a securității efective și reale*[9], o **nouă abordare privind gestionarea datelor** în materie de frontiere, securitate și gestionare a migrației, în care toate sistemele centralizate de informații ale UE în materie de securitate, frontiere și gestionare a migrației trebuie să fie interoperabile și să respecte pe deplin drepturile fundamentale. Comisia și-a anunțat intenția de a depune în continuare eforturi pentru a crea un portal european de căutare care să permită interogarea simultană a tuturor sistemelor UE relevante în domeniile securității, frontierelor și gestionării migrației, eventual cu norme mai simplificate de acces în scopul asigurării respectării legii, și pentru a dezvolta, pentru aceste sisteme, un serviciu comun de comparare a datelor biometrice (eventual cu o funcționalitate de marcare vizuală a

---

4 Rezoluția Parlamentului European din 6 iulie 2016 referitoare la prioritățile strategice ale programului de lucru al Comisiei pentru 2017 (2016/2773(RSP)).

5 Starea Uniunii 2016 (14.9.2016), https://ec.europa.eu/commission/state-union-2016_ro.

6 Concluziile Consiliului European (15.12.2016), http://www.consilium.europa.eu/ro/press/press-releases/2016/12/15/euco-conclusions-final/.

7 Decizia Comisiei din 17 iunie 2016 de instituire a Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate – 2016/C 257/03.

8 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

9 COM(2017) 261 final.

rezultatelor pozitive[10]) și un registru comun de date de identitate. De asemenea, Comisia și-a anunțat intenția de a prezenta, cât mai curând posibil, o propunere legislativă privind interoperabilitatea.

Concluziile Consiliului European din iunie 2017[11] au reiterat necesitatea luării de măsuri. Pornind de la concluziile din iunie 2017 ale Consiliului Justiție și Afaceri Interne[12], Consiliul European a invitat Comisia să elaboreze, cât mai curând posibil, un proiect legislativ care să includă recomandările formulate de grupul de experți la nivel înalt. Această inițiativă răspunde, de asemenea, solicitării Consiliului pentru un cadru global privind accesul în scopul asigurării respectării legii la diferitele baze de date în domeniul justiției și afacerilor interne, în vederea unei mai mari simplificări, coerențe, eficacități și concentrări asupra nevoilor operaționale[13]. Pentru a consolida eforturile de a face din Uniunea Europeană o societate mai sigură, cu respectarea deplină a drepturilor fundamentale, Comisia a anunțat, în cadrul programului său de lucru pentru 2018[14], că, până la sfârșitul anului 2017, urmează să prezinte o propunere privind interoperabilitatea sistemelor de informații.

- **Obiectivele propunerii**

Obiectivele generale ale acestei inițiative rezultă din obiectivele înscrise în tratat privind îmbunătățirea gestionării frontierelor externe ale spațiului Schengen și contribuția la securitatea internă a Uniunii Europene. Aceste obiective sunt, de asemenea, rezultatul deciziilor politice ale Comisiei și al concluziilor Consiliului (European) relevant. Aceste obiective sunt prezentate în detaliu în Agenda europeană privind migrația și în comunicările ulterioare, inclusiv în Comunicarea privind menținerea și consolidarea spațiului Schengen[15], în Agenda europeană privind securitatea[16] și în rapoartele Comisiei privind progresele înregistrate către o uniune a securității efectivă și autentică[17].

Deși se bazează în special pe comunicarea din aprilie 2016 și pe concluziile grupului de experți la nivel înalt, obiectivele prezentei propuneri sunt legate în mod intrinsec de documentele invocate mai sus.

Obiectivele specifice ale propunerii sunt următoarele:

(1) să asigure **accesul rapid, continuu, sistematic și controlat** al utilizatorilor finali, în special al polițiștilor de frontieră, al agenților responsabili cu aplicarea legii, al funcționarilor din cadrul serviciilor de imigrație și al autorităților judiciare, la informațiile de care au nevoie pentru a-și îndeplini sarcinile;

---

[10] Un nou concept de protejare a vieții private începând cu momentul conceperii, care restricționează accesul la ansamblul datelor, limitându-l la primirea unei simple notificări în cazul unui rezultat pozitiv/negativ, în care se indică prezența (sau absența) datelor.

[11] Concluziile Consiliului European, 22-23 iunie 2017.

[12] Rezultatele celei de a 3546-a reuniuni a Consiliului Justiție și Afaceri Interne din 8-9 iunie 2017, 10136/17.

[13] După ce a acordat Președinției Consiliului un mandat privind începerea negocierilor interinstituționale referitoare la sistemul de intrare/ieșire al UE la 2 martie 2017, Comitetul Reprezentanților Permanenți (Coreper) din cadrul Consiliului a aprobat un proiect de declarație a Consiliului prin care Comisia era invitată să propună un cadru global pentru accesul în scopul asigurării respectării legii la diferitele baze de date în domeniul justiției și afacerilor interne, în vederea unei mai mari simplificări, coerențe, eficacități și concentrări asupra nevoilor operaționale (Procesul verbal 7177/17, 21.3.2017).

[14] COM(2017)650 final.

[15] COM(2017)570 final.

[16] COM(2015)185 final.

[17] COM(2016)230 final.

(2) să ofere o soluție pentru **detectarea identităților multiple** legate de același set de date biometrice, care să faciliteze identificarea corectă a persoanelor de bună credință și **să combată fraudele de identitate**;

(3) să faciliteze **controalele de identitate efectuate asupra resortisanților țărilor terțe** pe teritoriul unui stat membru, de către autoritățile polițienești și

(4) să faciliteze și **să simplifice accesul autorităților de aplicare a legii** la sistemele de informații de la nivelul UE care nu intră în sfera asigurării respectării legii, atunci când acest lucru este necesar pentru prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor grave și a infracțiunilor de terorism.

În plus față de aceste obiective operaționale principale, prezenta propunere contribuie, de asemenea, la:

- facilitarea **implementării** din punct de vedere tehnic și operațional **de către statele membre** a sistemelor de informații actuale și viitoare;
- consolidarea și raționalizarea **condițiilor de asigurare a securității și a protecției datelor** care sunt aplicate în sistemele de informații respective și
- îmbunătățirea și armonizarea cerințelor în materie de **calitate a datelor** aplicate în sistemele respective.

În cele din urmă, prezenta propunere include dispoziții pentru instituirea și guvernanța formatului universal pentru mesaje, *Universal Message Format* – (UMF) ca standard UE pentru dezvoltarea sistemelor de informații în domeniul justiției și afacerilor interne, precum și instituirea unui registru central de raportare și statistici.

- **Domeniul de aplicare al propunerii**

Împreună cu cealaltă propunere din pachet prezentată în aceeași zi, prezenta propunere privind interoperabilitatea se concentrează asupra interoperabilității sistemelor de informații ale UE privind securitatea, frontierele și gestionarea migrației, care sunt exploatate la nivel central: trei care există deja, unul în curs de instituire, iar alte două în stadiu de propunere, în curs de dezbatere la nivel de colegiuitori. Fiecare sistem are propriile obiective, scopuri, temeiuri juridice, grupuri de utilizatori și propriul context instituțional.

Cele trei sisteme centralizate de informații existente în prezent sunt:

- **Sistemul de informații Schengen (SIS)**, care conține un spectru larg de semnalări referitoare la persoane (refuzuri de intrare sau de ședere în UE, mandatul european de arestare, persoane dispărute, asistență în cadrul procedurilor judiciare, controale discrete și specifice) și obiecte (inclusiv documente de identitate sau de călătorie pierdute, furate și anulate)[18];
- sistemul **Eurodac**, care cuprinde datele dactiloscopice ale solicitanților de azil și ale resortisanților țărilor terțe care au trecut frontierele externe în mod neregulamentar sau care se află în situație de ședere ilegală într-un stat membru și

[18] În proiectele de regulamente privind SIS prezentate de Comisie în decembrie 2016, se propune extinderea în continuare a acestui sistem, pentru a include deciziile de returnare și verificările prin interviu.

- **Sistemul de informații privind vizele (VIS)**, care cuprinde date privind vizele de scurtă ședere.

În plus față de aceste sisteme, Comisia a propus, în perioada 2016-2017, crearea a trei noi sisteme de informații gestionate centralizat la nivelul UE:

- **Sistemul de intrare/ieșire (EES)**, al cărui temei juridic tocmai a fost convenit, care va înlocui actualul sistem de ștampilare manuală a pașapoartelor și cu ajutorul căruia se vor înregistra electronic numele, tipul de document de călătorie, datele biometrice, precum și data și locul de intrare și de ieșire a resortisanților țărilor terțe care intră în spațiul Schengen pentru o ședere de scurtă durată;
- **Sistemul european de informații și de autorizare privind călătoriile (ETIAS)**, care se află în stadiu de propunere și care, odată ce va fi adoptat, va fi un sistem în mare parte automatizat care ar urma să colecteze și să verifice informațiile prezentate de resortisanții țărilor terțe exonerați de obligația de a deține viză înainte de a călători în spațiul Schengen și
- **Sistemul european de informații cu privire la cazierele judiciare ale resortisanților țărilor terțe (ECRIS-TCN)**, aflat în stadiu de propunere, care va fi un sistem electronic ce va permite schimbul de informații privind condamnările anterioare pronunțate împotriva resortisanților țărilor terțe de către instanțele penale din UE.

Aceste șase sisteme sunt complementare și – cu excepția Sistemului de informații Schengen (SIS) – îi vizează exclusiv pe resortisanții țărilor terțe. Sistemele sprijină autoritățile naționale în activitatea de gestionare a frontierelor, a migrației, în procesul de prelucrare a cererilor de viză și de azil, precum și în combaterea criminalității și a terorismului. În ceea ce privește acest ultim aspect, se aplică în special SIS, care este instrumentul de schimb de informații cel mai utilizat în prezent în scopul asigurării respectării legii.

În plus față de aceste sisteme de informații, gestionate centralizat la nivelul UE, prezenta propunere vizează, de asemenea, baza de date a **Interpol** privind documentele de călătorie furate și pierdute (SLTD), în care, în conformitate cu dispozițiile din Codul frontierelor Schengen, se fac căutări în mod sistematic la frontierele externe ale UE, și baza de date a Interpol privind documentele de călătorie asociate unor notificări (TDAWN). Propunerea vizează, de asemenea, datele **Europol**, în măsura în care acest lucru este relevant pentru funcționarea sistemului ETIAS propus, pentru a ajuta statele membre să interogheze bazele de date pentru infracțiuni grave și acte de terorism.

Sistemele de informații naționale și sistemele de informații UE descentralizate nu fac obiectul prezentei inițiative. Dacă se va dovedi că acest lucru este necesar, se prevede posibilitatea ca sistemele descentralizate, precum cele operate în temeiul Tratatului de la Prüm[19], al Directivei privind registrul cu numele pasagerilor (PNR)[20] și al Directivei privind informațiile prealabile referitoare la pasageri[21], să fie, într-un stadiu ulterior, conectate la una sau mai multe dintre componentele propuse în prezenta inițiativă[22].

---

19 http://eur-lex.europa.eu/legal-content/ro/TXT/?qid=1508936184412&uri=CELEX:32008D0615.

20 http://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1508936384641&uri=CELEX:32016L0681.

21 Directiva 2004/82/CE a Consiliului din 29 aprilie 2004 privind obligația operatorilor de transport de a comunica datele privind pasagerii.

22 În mod similar, în ceea ce privește sistemele vamale, Consiliul a invitat Comisia, în concluziile sale din iunie 2017, să realizeze un studiu de fezabilitate în care să analizeze în profunzime aspectele tehnice, operaționale și juridice pe care le presupune asigurarea interoperabilității sistemelor de securitate și de gestionare a frontierelor cu sistemele

Pentru a respecta deosebirea dintre elementele care constituie o dezvoltare a acquis-ului Schengen privind frontierele și vizele, pe de o parte, și celelalte sisteme care se referă la acquis-ul Schengen privind cooperarea polițienească sau care nu sunt legate de acquis-ul Schengen, pe de altă parte, prezenta propunere face referire la accesul la Sistemul de informații privind vizele, la Sistemul de informații Schengen, reglementat în prezent prin Regulamentul (CE) nr. 1987/2006, la Sistemul de intrare/ieșire și la Sistemul european de informații și de autorizare privind călătoriile.

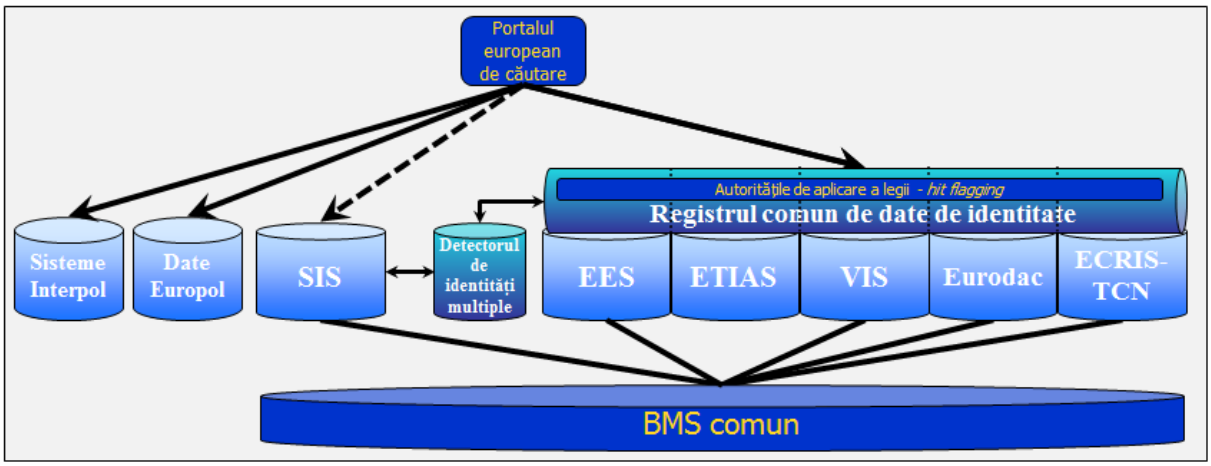
- **Componentele tehnice necesare pentru realizarea interoperabilității**

Pentru a atinge obiectivele prezentei propuneri, trebuie instituite patru componente necesare pentru asigurarea interoperabilității:

- portalul european de căutare – ESP
- serviciul comun de comparare a datelor biometrice – BMS comun
- registrul comun de date de identitate – CIR
- detectorul de identități multiple – MID.

Fiecare dintre aceste componente este descrisă în detaliu în documentul de lucru al serviciilor Comisiei privind evaluarea impactului, care însoțește prezenta propunere.

Combinarea celor patru componente conduce la următoarele soluții de interoperabilitate:



Obiectivele și funcționarea acestor patru elemente pot fi sintetizate după cum urmează:

(1) **Portalul european de căutare (ESP)** este componenta care va permite interogarea simultană a mai multor sisteme (SIS central, Eurodac, VIS, viitorul EES, sistemele ETIAS și ECRIS-TCN, ambele aflate în stadiu de propunere, și sistemele de date relevante ale Interpol și datele Europol) utilizând datele de identitate (atât cele biografice, cât și cele biometrice). Portalul va garanta accesul rapid, fără sincope, eficient, sistematic și controlat al utilizatorilor sistemelor de informații ale UE la toate informațiile de care au nevoie pentru a-și îndeplini sarcinile.

Printr-o interogare lansată pe portalul european de căutare, utilizatorul va obține imediat, în câteva secunde, informații din diferitele sisteme la care are acces legal. În funcție de scopul

vamale și să prezinte rezultatele acestui studiu până la sfârșitul anului 2018, în vederea discutării acestuia în cadrul Consiliului.

interogării și de drepturile de acces corespunzătoare, urmează să se prevadă configurații specifice în ESP.

ESP nu prelucrează date noi și nu stochează niciun fel de date; acesta urmează să funcționeze ca un ghișeu unic sau ca un „broker de mesaje” prin care se vor lansa interogări în diverse sisteme centrale și se vor extrage fără probleme informațiile necesare, cu respectarea deplină a cerințelor privind controlul accesului și protecția datelor care se aplică sistemelor de bază. ESP va facilita utilizarea corectă și autorizată a fiecăruia dintre sistemele de informații existente la nivelul UE, iar consultarea și utilizarea sistemelor va fi mai ușoară și mai puțin costisitoare pentru statele membre, cu respectarea instrumentelor juridice care guvernează aceste sisteme.

(2) **Serviciul comun de comparare a datelor biometrice (BMS comun)** va permite efectuarea de interogări și compararea datelor biometrice (amprente digitale și imagini faciale) din mai multe sisteme centrale (în special SIS, Eurodac, VIS, viitorul EES și sistemul ECRIS-TCN, aflat în stadiu de propunere). Sistemul ETIAS, aflat în stadiu de propunere, nu va conține date biometrice și, prin urmare, nu va fi legat la BMS comun.

Dacă în prezent fiecare sistem central existent (SIS, Eurodac, VIS) are un motor de căutare propriu, specific, pentru datele biometrice[23], serviciul comun de comparare a datelor biometrice urmează să ofere o platformă comună care va permite interogarea și compararea simultană a datelor. BMS comun va genera beneficii substanțiale în ceea ce privește securitatea, costurile, întreținerea și exploatarea, bazându-se pe o componentă tehnologică unică în loc de cinci. Datele biometrice (amprente digitale și imagini faciale) sunt stocate exclusiv de sistemele consultate. BMS comun va crea și păstra o reprezentare matematică a eșantioanelor biometrice (un model), fără să păstreze însă efectiv datele, care rămân astfel stocate într-un singur loc, o singură dată.

BMS comun va fi un instrument esențial pentru identificarea conexiunilor dintre seturile de date și diferitele identități asumate de aceeași persoană în diferite sisteme centrale. Fără un BMS comun, niciuna dintre celelalte trei componente nu va putea funcționa.

(3) **Registrul comun de date de identitate (CIR)** va fi componenta comună pentru stocarea datelor biografice[24] și biometrice de identitate ale resortisanților țărilor terțe înregistrate în Eurodac, în VIS și în viitorul sistem EES, precum și în ETIAS și în sistemul ECRIS-TCN, ambele aflate în stadiu de propunere). Fiecare dintre aceste cinci sisteme centrale înregistrează sau va înregistra datele biografice referitoare la anumite persoane în scopuri specifice. Acest lucru nu se va schimba. Datele de identitate relevante vor fi stocate în CIR, însă vor „aparține” în continuare sistemelor de bază în care sunt înregistrate datele respective.

CIR nu va conține date SIS. Din cauza arhitecturii tehnice complexe a SIS, care conține copii naționale, copii naționale parțiale și eventuale sisteme naționale de comparare a datelor biometrice, dacă ar integra și datele SIS, CIR ar deveni atât de complex, încât ar putea să nu mai fie viabil din punct de vedere tehnic și financiar.

Obiectivul principal al CIR este de a facilita identificarea biografică a resortisanților țărilor terțe. Datorită acestui registru, va crește viteza operațiunilor, se va îmbunătăți eficiența și se vor

[23] Din punct de vedere tehnic, aceste motoare de căutare a datelor biometrice sunt cunoscute sub denumirea de sistem automat de identificare a amprentelor digitale (AFIS) sau de sistem automat de identificare biometrică (ABIS).

[24] Pe documentul de călătorie pot figura date biografice precum: numele de familie, prenumele, sexul, data nașterii, numărul documentului de călătorie, dar nu și adresa, numele anterioare, datele biometrice etc.

face economii de scară. Instituirea CIR este necesară pentru verificarea eficace a identității resortisanților țărilor terțe, inclusiv a celor aflați pe teritoriul unui stat membru. În plus, prin adăugarea unei funcționalități de marcare vizuală a rezultatelor pozitive în CIR, se va putea verifica dacă există sau nu date în oricare dintre sistemele legate la CIR prin transmiterea unei simple notificări în cazul unui rezultat pozitiv/negativ. În acest mod, CIR va contribui, de asemenea, la raționalizarea accesului autorităților de aplicare a legii la sistemele de informații care nu intră în sfera asigurării respectării legii, menținând totodată un nivel ridicat de protecție a datelor (a se vedea, mai jos, secțiunea privind abordarea în două etape a accesului în scopul asigurării respectării legii).

Dintre cele cinci sisteme care urmează să facă parte din CIR, atât viitorul EES, cât și sistemele ETIAS și ECRIS-TCN – ultimele două fiind în stadiu de proiect – sunt sisteme noi care urmează să fie dezvoltate. Actualul Eurodac nu conține date biografice; această componentă se va dezvolta imediat după adoptarea noului temei juridic pentru Eurodac. Actualul VIS conține date biografice, dar interacțiunile necesare între VIS și viitorul EES vor necesita o modernizare a sistemului VIS existent. Așadar, CIR va fi înființat la momentul potrivit. În niciun caz crearea CIR nu va însemna duplicarea datelor existente. Din punct de vedere tehnic, CIR va fi creat pe baza platformei EES/ETIAS.

(4) **Detectorul de identități multiple (MID)** va verifica dacă datele de identitate căutate există în mai multe sisteme conectate la acesta. MID efectuează căutări atât în sistemele care stochează date de identitate în CIR (Eurodac, VIS, viitorul EEAS, sistemul ETIAS și sistemul ECRIS-TCN - ultimele două aflate în stadiu de propunere), cât și în SIS. MID va permite detectarea identităților multiple legate de același set de date biometrice, pentru a asigura identificarea corectă a persoanelor de bună credință și pentru a combate fraudele de identitate.

Cu ajutorul MID se va putea stabili dacă nume diferite corespund unei singure identități. Acest element de noutate este necesar pentru a aborda în mod eficace problema utilizării frauduloase a identității, care reprezintă o încălcare gravă a securității. MID va evidenția doar datele biografice de identitate pentru care există o conexiune în diferitele sisteme centrale. Aceste conexiuni vor fi detectate utilizându-se serviciul comun de comparare a datelor biometrice pe baza datelor biometrice și vor trebui confirmate sau respinse de autoritatea care a înregistrat datele în sistemul de informații ce a condus la stabilirea conexiunii. Pentru a oferi asistență utilizatorilor autorizați ai MID în îndeplinirea acestei sarcini, sistemul va trebui să eticheteze conexiunile identificate, împărțindu-le în patru categorii:

- Conexiunea galbenă – posibilitatea existenței unor identități biografice care pot fi diferite referitoare la aceeași persoană;
- Conexiunea albă – confirmarea faptului că identitățile biografice diferite aparțin aceleiași persoane de bună credință;
- Conexiunea verde – confirmarea faptului că persoane de bună credință diferite au aceeași identitate biografică;
- Conexiunea roșie – suspiciunea că o anumită persoană utilizează în mod ilegal diferite identități biografice.

Prezenta propunere descrie procedurile care vor fi instituite pentru gestionarea acestor categorii diferite. Ambiguitatea legată de identitatea persoanelor de bună credință ar trebui înlăturată cât mai repede posibil, transformând conexiunea galbenă într-o conexiune verde sau albă

confirmată, astfel încât să se garanteze faptul că aceste persoane nu se vor confrunta cu probleme inutile. Pe de altă parte, atunci când în urma evaluării se confirmă o conexiune roșie sau o conexiune galbenă se modifică în una roșie, se impune luarea unor măsuri corespunzătoare.

- **Abordarea în două etape a accesului în scopul asigurării respectării legii, astfel cum este prevăzută în registrul comun de date de identitate**

Asigurarea respectării legii este definită ca un obiectiv secundar sau accesoriu al Eurodac, al VIS, al viitorului EES și al sistemului ETIAS, aflat în stadiu de propunere. Prin urmare, posibilitatea de a accesa datele stocate în aceste sisteme în scopul asigurării respectării legii este limitată. Autoritățile de aplicare a legii pot consulta direct aceste sisteme de informații care nu intră în sfera asigurării respectării legii exclusiv în scopul prevenirii, depistării, investigării sau urmăririi penale a actelor de terorism și a altor infracțiuni grave. În plus, condițiile de acces și garanțiile aplicabile diferă de la un sistem la altul, iar o parte din normele aflate în vigoare ar putea încetini utilizarea legitimă a sistemelor de către aceste autorități. La un nivel mai general, principiul căutării prealabile limitează posibilitatea autorităților statelor membre de a consulta sistemele în scopuri justificate de asigurare a respectării legii, iar acest lucru ar putea duce la situații în care se ratează ocazia de a scoate la lumină informațiile necesare.

În comunicarea sa din aprilie 2016, Comisia a recunoscut necesitatea optimizării instrumentelor existente în scopul asigurării respectării legii, respectându-se, în același timp, cerințele privind protecția datelor cu caracter personal. Această necesitate a fost confirmată și reiterată de către statele membre și agențiile relevante în cadrul grupului de experți la nivel înalt.

Având în vedere cele de mai sus, prin dotarea CIR cu o funcționalitate de marcare vizuală a rezultatelor pozitive, prezenta propunere introduce posibilitatea de accesare a EES, Eurodac și VIS, ETIAS și Eurodac utilizând **o abordare în două etape de consultare a datelor**. Această abordare în două etape nu va schimba faptul că aplicarea legii este un obiectiv strict accesoriu al acestor sisteme și, prin urmare, ar trebui să se respecte norme stricte de acces.

Într-o primă etapă, un agent responsabil cu aplicarea legii va efectua o interogare referitoare la o anumită persoană folosind datele de identitate, documentul de călătorie sau datele biometrice ale persoanei respective, pentru a verifica dacă informațiile privind persoana căutată sunt stocate în CIR. În cazul în care aceste date sunt prezente, reprezentantul respectiv va primi **un răspuns în care se indică care dintre sistemele de informații ale UE conține date** referitoare la această persoană (**marcaj vizual al rezultatelor pozitive**). Reprezentantul autorității de aplicare a legii nu va avea acces efectiv la datele din niciunul dintre sistemele de bază.

În a doua etapă, reprezentantul poate solicita acces la fiecare dintre sistemele în care au fost identificate date, în vederea obținerii întregului dosar al persoanei căutate, **în conformitate cu normele și procedurile stabilite pentru fiecare sistem în parte**. Această a doua etapă de acces va fi în continuare condiționată de primirea unei autorizări prealabile din partea unei autorități desemnate și de utilizarea unui anumit nume de utilizator (ID), cu consemnarea într-un registru a consultărilor respective.

Această nouă abordare va aduce o valoare adăugată autorităților de aplicare a legii datorită **existenței unor posibile conexiuni** în MID. MID va ajuta CIR să identifice conexiunile existente, astfel încât rezultatele obținute vor fi mai precise. MID va fi în măsură să precizeze dacă persoana este **cunoscută cu identități diferite** în diverse sisteme de informații.

Consultarea datelor în două etape este deosebit de importantă în cazurile în care suspecții, autorii sau victimele unei infracțiuni de terorism sau ale unei alte infracțiuni grave **sunt necunoscuți**. În aceste cazuri, CIR va permite, de fapt, identificarea sistemului de informații care conține date referitoare la persoana respectivă printr-o singură căutare. Procedând astfel, actualele condiții care impun efectuarea, în prealabil, a unor căutări în bazele de date naționale și a unei căutări prealabile în sistemul de identificare automată a amprentelor digitale al altor state membre, în temeiul Deciziei 2008/615/JAI („verificarea Prüm”), devin redundante.

Noua abordare, care constă în consultarea datelor în două etape, **va intra în vigoare** numai **după ce componentele necesare pentru asigurarea interoperabilității vor fi pe deplin operaționale**.

- **Elemente suplimentare din prezenta propunere care pot veni în sprijinul componentelor necesare pentru asigurarea interoperabilității**

(1) Pe lângă componentele menționate mai sus, prezentul proiect de regulament include, de asemenea, propunerea de instituire a unui **registru central de raportare și statistici (CRRS)**. Acest registru este necesar pentru a permite crearea și schimbul de rapoarte conținând date statistice (anonime) în scopuri strategice, operaționale și de asigurare a calității datelor. Practica actuală de colectare a datelor statistice numai din sistemele de informații separate afectează securitatea datelor și calitatea rezultatelor și nu permite corelarea datelor între diversele sisteme.

CRRS va servi drept depozit de date specific și distinct pentru statisticile anonime extrase din SIS, VIS, Eurodac, viitorul EES și sistemele ETIAS și ECRIS-TCN – ambele aflate în stadiu de propunere –, din registrul comun de date de identitate, din detectorul de identități multiple și din serviciul comun de comparare a datelor biometrice. Registrul va oferi statelor membre, Comisiei (inclusiv Eurostat) și agențiilor UE posibilitatea a face schimb de rapoarte în condiții de securitate (potrivit dispozițiilor incluse în instrumentele juridice respective).

Crearea unui registru central în loc de mai multe registre separate, unul pentru fiecare sistem, va presupune costuri mai mici și va necesita eforturi mai puține pentru crearea, exploatarea și întreținerea acestuia. De asemenea, aceasta va asigura un nivel mai ridicat de securitate a datelor, pentru că datele vor fi stocate într-un registru unic, iar control accesului se va limita la acest registru.

(2) Prezentul proiect de regulament propune, de asemenea, crearea **formatului universal pentru mesaje (UMF)** ca standard ce va fi utilizat la nivelul UE pentru a orchestra interacțiunile dintre mai multe sisteme într-un mod interoperabil, inclusiv sistemele dezvoltate și gestionate de eu-LISA. Mai mult, Europol și Interpol vor fi încurajate să folosească acest standard.

Standardul UMF introduce un limbaj tehnic comun și unitar pentru a descrie elementele de date și a le pune în relație, în special elementele referitoare la persoane și la documente (de călătorie). Utilizarea UMF pentru elaborarea de noi sisteme de informații facilitează integrarea și interoperabilitatea cu alte sisteme, în special pentru statele membre care trebuie să creeze interfețe de comunicare cu aceste sisteme noi. În acest sens, utilizarea obligatorie a UMF pentru crearea de sisteme noi poate fi considerată o condiție prealabilă necesară pentru introducerea componentelor necesare pentru asigurarea interoperabilității propuse în prezentul regulament.

Pentru a se asigura aplicarea standardului UMF la nivelul întregii UE, se propune o structură de guvernanță adecvată. Comisia va fi responsabilă cu crearea și dezvoltarea standardului UMF în cadrul unei proceduri de examinare cu statele membre, la care vor participa și statele membre

asociate Schengen, agențiile UE și organismele internaționale participante la proiectele UMF (precum eu-LISA, Europol și Interpol). Structura de guvernanță propusă este de importanță vitală pentru extinderea și dezvoltarea UMF, garantând în același timp condiții optime de utilizare și aplicabilitate a acestui standard.

(3) Prezentul proiect de regulament introduce conceptele de **mecanisme de control automatizat al calității datelor** și indicatori comuni de calitate, precum și necesitatea asigurării celui mai înalt nivel de calitate a datelor de către statele membre atunci când sistemele cu date și utilizează sistemele respective. Dacă datele nu sunt de cea mai înaltă calitate, pot exista consecințe nu doar în ceea ce privește identificarea persoanelor căutate, ci și în ceea ce privește drepturile fundamentale ale persoanelor nevinovate. Introducerea datelor de către operatori umani poate da naștere unor probleme care pot fi evitate prin introducerea unor norme de validare automată. Scopul ar fi acela de a identifica în mod automat datele care par a fi incorecte sau inconsecvente, astfel încât statul membru de unde provin să fie în măsură să le verifice și să ia măsurile necesare pentru a le corecta. La toate acestea se adaugă rapoartele periodice privind calitatea datelor elaborate de eu-LISA.

- **Consecințele asupra altor instrumente juridice**

Împreună cu cealaltă propunere care face parte din acest pachet, prezentul proiect de regulament introduce inovații care vor necesita modificarea altor instrumente juridice:

- Regulamentul (UE) nr. 2016/399 (Codul Frontierelor Schengen)
- Regulamentul (UE) nr. 2017/2226 (Regulamentul EES)
- Regulamentul (CE) nr. 767/2008 (Regulamentul VIS)
- Decizia 2004/512/CE a Consiliului (Decizia VIS)
- Decizia 2008/633/JAI a Consiliului (Decizia privind accesul autorităților de aplicare a legii la VIS)
- [Regulamentul ETIAS]
- [Regulamentul Eurodac]
- [Regulamentele SIS]
- [Regulamentul ECRIS-TCN, inclusiv dispozițiile corespunzătoare din Regulamentul (UE) 2016/1624 (Regulamentul privind poliția de frontieră și garda de coastă)]
- [Regulamentul eu-LISA].

Prezenta propunere și cealaltă propunere care face parte din acest pachet includ, de asemenea, dispoziții detaliate privind modificările care trebuie aduse instrumentelor juridice care sunt în prezent texte stabile, în forma adoptată de colegiuitori: Codul frontierelor Schengen, Regulamentul EES, Regulamentul VIS, Decizia 2008/633/JAI a Consiliului și Decizia 2004/512/CE a Consiliului.

Celelalte instrumente enumerate (Regulamentele ETIAS, Eurodac, SIS, ECRIS-TCN, eu-LISA) sunt în curs de negociere în cadrul Parlamentului European și al Consiliului. Pentru aceste instrumente, este, așadar, imposibil, în această etapă, să se prevadă modificările necesare. Comisia va prezenta astfel de modificări pentru fiecare dintre aceste instrumente în termen de două săptămâni din momentul în care se va ajunge la un acord politic cu privire la proiectele de regulamente respective.

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

Prezenta propunere se înscrie în cadrul unui proces mai larg, care a fost lansat prin comunicarea din aprilie 2016 intitulată *„Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”* și prin activitatea ulterioară a Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate. Propunerea vizează îndeplinirea a trei obiective:

(a) să consolideze și să maximizeze beneficiile **sistemelor de informații existente**;

(b) să acopere lacunele în materie de informații prin instituirea unor noi sisteme de informații;

(c) să consolideze interoperabilitatea acestor sisteme.

În ceea ce privește primul obiectiv, Comisia a adoptat, în decembrie 2016, propuneri menite să consolideze în continuare actualul Sistem de informații Schengen (SIS)[25]. În ceea ce privește Eurodac, în urma propunerii Comisiei din mai 2016[26], s-a înregistrat o accelerare a negocierilor privind temeiul juridic revizuit al acestuia. O propunere referitoare la un nou temei juridic pentru Sistemul de informații privind vizele (VIS) este, de asemenea, în curs de elaborare și urmează să fie prezentată în cel de al doilea trimestru al anului 2018.

În ceea ce privește cel de al doilea obiectiv, negocierile privind propunerea Comisiei din aprilie 2016 privind instituirea Sistemului de intrare/ieșire (EES)[27] s-au încheiat încă din iulie 2017, când colegiuitorii au ajuns la un acord politic, confirmat de Parlamentul European în octombrie 2017 și adoptat de Consiliu în noiembrie 2017. Temeiul juridic va intra în vigoare în decembrie 2017. Au început negocierile pe marginea propunerii din noiembrie 2016 privind instituirea sistemului european de informații și de autorizare privind călătoriile (ETIAS)[28], acestea urmând a fi finalizate în lunile următoare. În iunie 2017, Comisia a propus un temei juridic pentru a acoperi o altă lacună la nivel de informații: sistemul european de informații cu privire la cazierele judiciare ale resortisanților țărilor terțe (sistemul ECRIS-TCN)[29]. Și în acest caz, colegiuitorii au precizat că intenționează să adopte rapid acest temei juridic.

Prezenta propunere abordează cel de al treilea obiectiv identificat în comunicarea din aprilie 2016.

- **Coerența cu celelalte politici ale Uniunii în domeniul justiției și al afacerilor interne**

Atât prezenta propunere, cât și cealaltă propunere din pachet respectă și urmează liniile trasate în Agenda europeană privind migrația și în comunicările ulterioare, inclusiv în Comunicarea privind menținerea și consolidarea spațiului Schengen[30], în Agenda europeană privind securitatea[31] și în activitatea și rapoartele Comisiei privind progresele înregistrate către o uniune a securității efectivă și autentică[32]. Prezenta propunere este coerentă cu alte politici ale Uniunii, și anume:

- securitatea internă: Agenda europeană privind securitatea prevede că respectarea unor standarde comune ridicate în materie de gestionare a frontierelor este esențială pentru

[25] COM(2016) 883 final.
[26] COM(2016) 272 final.
[27] COM(2016) 194 final.
[28] COM(2016) 731 final.
[29] COM(2017) 344 final.
[30] COM(2017)570 final.
[31] COM(2015)185 final.
[32] COM(2016)230 final.

prevenirea criminalității transfrontaliere și a terorismului. Prezenta propunere contribuie la realizarea unui nivel ridicat de securitate internă, oferindu-le autorităților mijloacele necesare pentru accesarea rapidă, fără sincope, sistematică și controlată a informațiilor de care au nevoie.

- azilul: propunerea include Eurodac printre sistemele centrale ale UE care vor beneficia de interoperabilitate.
- gestionarea frontierelor externe și securitatea: prezenta propunere consolidează sistemele SIS și VIS, care contribuie la controlul eficient al frontierelor externe ale Uniunii, viitorul EES, precum și sistemele ETIAS și ECRIS-TCN, ambele aflate în stadiu de propunere.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

• Temei juridic

Principalul temei juridic va fi constituit din următoarele articole din Tratatul privind funcționarea Uniunii Europene: articolul 16 alineatul (2), articolul 74, articolul 77 alineatul (2) literele (a), (b), (d) și (e).

În temeiul articolului 16 alineatul (2), Uniunea are competența de a adopta măsuri referitoare la protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii, precum și de către statele membre atunci când desfășoară activități care fac parte din domeniul de aplicare a dreptului Uniunii, precum și de a adopta norme privind libera circulație a acestor date. În temeiul articolului 74, Consiliul poate să adopte măsuri în vederea asigurării cooperării administrative între departamentele din statele membre în domeniul justiției, libertății și securității. În temeiul articolului 77 alineatul (2) literele (a), (b), (d) și (e), Parlamentul European și Consiliul pot adopta măsuri privind politica comună a vizelor și a altor permise de ședere de scurtă durată, controalele la care sunt supuse persoanele la trecerea frontierelor externe, orice măsură necesară pentru instituirea treptată a unui sistem integrat de administrare a frontierelor externe și absența oricărui control asupra persoanelor, indiferent de cetățenie, la trecerea frontierelor interne.

• Subsidiaritate

Libertatea de mișcare în cadrul UE necesită gestionarea eficace a frontierelor externe ale Uniunii în vederea garantării securității. Statele membre au convenit, prin urmare, să abordeze aceste provocări în mod colectiv, în special făcând schimb de informații prin sisteme centralizate la nivelul UE în domeniul justiției și afacerilor interne. Acest lucru este confirmat de diferitele concluzii care au fost adoptate atât de Consiliul European, cât și de Consiliu, mai ales începând din 2015.

Absența controalelor la frontierele interne impune o gestionare eficace a frontierelor externe ale spațiului Schengen, fiecare stat membru sau țară asociată spațiului Schengen având îndatorirea de a controla frontierele externe în numele celorlalte state Schengen. Prin urmare, niciun stat membru nu este capabil să facă față singur migrației neregulamentare și criminalității transfrontaliere. Resortisanții țărilor terțe care intră în spațiul fără controale la frontierele interne pot circula liber în cadrul acestuia. Într-un spațiu fără frontiere interne, toate acțiunile de combatere a imigrației neregulamentare și a criminalității și terorismului internațional, inclusiv prin detectarea fraudelor de identitate, ar trebui întreprinse în comun; aceste aspecte pot fi abordate cu succes doar la nivelul UE.

Principalele sisteme de informații comune la nivelul UE au fost deja instituite sau sunt în curs de instituire. O mai mare interoperabilitate între aceste sisteme de informații implică în mod automat o acțiune la nivelul Uniunii. Elementul central al propunerii este îmbunătățirea eficienței și a utilizării

sistemelor centralizate gestionate de eu-LISA. Având în vedere amploarea, efectele și impactul acțiunilor preconizate, obiectivele sale fundamentale nu pot fi realizate în mod eficient și sistematic decât la nivelul UE.

- **Proporționalitate**

Astfel cum se explică în detaliu în evaluarea impactului care însoțește prezenta propunere de regulament, alegerile de politică din prezenta propunere sunt considerate proporționale. Acestea nu depășesc ceea ce este necesar pentru îndeplinirea obiectivelor stabilite.

Portalul european de căutare (ESP) este un instrument necesar pentru consolidarea utilizării autorizate a sistemelor de informații actuale și viitoare ale UE. Impactul ESP în ceea ce privește prelucrarea datelor este foarte limitat. Pe acest portal nu se vor stoca niciun fel de date, cu excepția informațiilor privind diferitele profiluri ale utilizatorilor ESP, a datelor și a sistemelor de informații la care au acces, activitatea acestora fiind monitorizată cu ajutorul istoricului de accesări. Rolul ESP de broker de mesaje, catalizator și facilitator este proporțional, necesar și limitat în ceea ce privește căutările și drepturile de acces astfel cum se prevede în temeiurile juridice referitoare la sistemele de informații și în propunerea de regulament privind interoperabilitatea.

Serviciul comun de comparare a datelor biometrice (BMS comun) este necesar pentru funcționarea ESP, a registrului comun de date de identitate și a detectorului de identități multiple și facilitează utilizarea și întreținerea sistemelor de informații relevante ale UE, atât a celor existente, cât și a celor viitoare. Funcționalitatea acestuia permite efectuarea de căutări eficiente, continue și sistematice privind datele biometrice din diverse surse. Datele biometrice sunt stocate și păstrate de către sistemele de bază. BMS comun creează modele, eliminând imaginile reale. Datele sunt stocate într-un singur loc și o singură dată.

Registrul comun de date de identitate (CIR) este necesar pentru identificarea corectă a unui resortisant al unei țări terțe, de exemplu în cursul unei verificări a identității în spațiul Schengen. CIR sprijină, de asemenea, funcționarea detectorului de identități multiple și este, prin urmare, un element necesar atât pentru facilitarea controalelor de identitate pentru călătorii de bună credință, cât și pentru combaterea fraudelor de identitate. Accesul la CIR în acest scop este limitat la utilizatorii care au nevoie de aceste informații pentru a-și îndeplini sarcinile (ceea ce înseamnă că aceste controale trebuie să devină o nouă funcție accesorie a Eurodac, VIS și a viitorului EES, precum și a sistemelor ETIAS și ECRIS-TCN, ambele aflate în stadiu de propunere). Prelucrarea datelor se limitează strict la ceea ce este necesar pentru atingerea acestui obiectiv; se vor introduce măsuri de protecție adecvate care să garanteze respectarea drepturilor de acces și reducerea la minimul necesar a datelor stocate în CIR. Pentru a se asigura reducerea la minimum a datelor și pentru a se evita duplicarea nejustificată a datelor, CIR păstrează datele biografice solicitate fiecăruia dintre sistemele sale de bază – stocate, modificate, adăugate sau eliminate în conformitate cu temeiurile juridice respective ale acestora – fără a le copia. Condițiile de păstrare a datelor sunt pe deplin aliniate cu dispozițiile în materie de păstrare a datelor aplicabile sistemelor de informații de bază care furnizează datele de identitate.

Detectorul de identități multiple (MID) este necesar pentru a oferi o soluție pentru detectarea identităților multiple care să asigure identificarea corectă a persoanelor de bună credință și să combată fraudele de identitate. MID va conține conexiunile dintre persoanele ale căror date sunt prezente în mai multe sisteme centrale de informații, care se limitează în mod strict la datele necesare pentru a verifica dacă o persoană este înregistrată în mod legal sau ilegal cu diferite identități biografice în sisteme diferite și pentru a clarifica dacă două persoane cu date biografice similare nu sunt, de fapt, aceeași persoană. Prelucrarea datelor prin intermediul MID și al BMS comun pentru a stabili conexiuni între dosarele individuale din diferite sisteme se limitează la

strictul necesar. MID va include garanții împotriva unor eventuale cazuri de discriminare sau a unor decizii nefavorabile care vizează persoane cu identități multiple legale.

- **Alegerea instrumentului**

Se propune adoptarea unui regulament al Parlamentului European și al Consiliului. Legislația propusă vizează în mod direct funcționarea sistemelor de informații în materie de frontiere și securitate gestionate centralizat la nivelul UE, dintre care unele au fost instituite, iar altele urmează să fie instituite prin regulamente. În mod asemănător, eu-LISA, agenția care va fi responsabilă cu conceperea și dezvoltarea componentelor și, în timp, de administrarea tehnică a acestora a fost, de asemenea, instituită printr-un regulament. Prin urmare, regulamentul este instrumentul adecvat.

3. REZULTATELE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRII IMPACTULUI

- **Consultarea publică**

În perspectiva prezentei propuneri, Comisia a lansat, în iulie 2017, o consultare publică pentru a cunoaște punctele de vedere ale părților interesate cu privire la interoperabilitate. În cadrul acestei consultări, Comisia a primit 18 răspunsuri de la diverse părți interesate, printre care se numără guverne ale unor state membre, organizații din sectorul privat, alte organizații precum ONG-uri și grupuri de reflecție, precum și cetățeni, care au răspuns în nume propriu[33]. În general, răspunsurile au fost, în mare parte, în favoarea principiilor care stau la baza prezentei propuneri privind interoperabilitatea. Marea majoritate a respondenților au fost de acord că problemele identificate în cadrul consultării și obiectivele urmărite în cadrul pachetului privind interoperabilitatea sunt cele corecte. Mai precis, respondenții consideră că, datorită opțiunilor prezentate în documentul de consultare:

- personalul de pe teren va avea acces la informațiile de care are nevoie;
- se va evita duplicarea datelor, se vor reduce suprapunerile și se vor pune în evidență discrepanțele dintre date;
- va crește fiabilitatea procedurii de identificare a persoanelor – inclusiv a persoanelor cu identități multiple – și va scădea numărul fraudelor de identitate.

O majoritate clară a respondenților au susținut fiecare dintre opțiunile propuse, considerându-le necesare pentru atingerea obiectivelor prezentei inițiative și subliniind, în răspunsurile lor, necesitatea adoptării unor măsuri puternice și clare de protecție a datelor, în special în ceea ce privește accesul la informațiile stocate în sisteme și păstrarea datelor, precum și necesitatea unor date actualizate de înaltă calitate în sisteme și a unor măsuri care să garanteze acest lucru.

Pentru pregătirea prezentei propuneri s-a ținut cont de toate punctele aduse în discuție.

- **Sondajul Eurobarometru**

În iunie 2017, s-a efectuat un sondaj special Eurobarometru[34], care arată că strategia UE privind schimbul de informații la nivelul UE în scopul combaterii criminalității și a terorismului se bucură

[33] Raportul de sinteză anexat la evaluarea impactului cuprinde detalii suplimentare în acest sens.

[34] În raportul intitulat *Report on Europeans' attitudes towards security* (Raport privind atitudinea europenilor față de securitate) se analizează rezultatele sondajului Eurobarometru special (464b) privind cunoștințele, experiențele și percepțiile generale ale cetățenilor legate de securitate. Acest sondaj a fost realizat de rețeaua TNS Political & Social în 28 de state membre în perioada 13-26 iunie 2017. Au fost intervievați aproximativ 28 093 de cetățeni UE din diverse categorii sociale și demografice.

de un sprijin puternic în rândul cetățenilor: aproape toți respondenții (92 %) sunt de acord că autoritățile naționale ar trebui să facă schimb de informații cu autoritățile din alte state membre pentru o mai bună combatere a criminalității și a terorismului.

Potrivit unei majorități clare a respondenților (69 %), poliția și alte autorități naționale de aplicare a legii ar trebui să facă în mod sistematic schimb de informații cu alte țări ale UE. În toate statele membre, majoritatea respondenților sunt de părere că ar trebui să existe un schimb de informații în fiecare caz în parte.

- **Grupul de experți la nivel înalt pentru sistemele de informații și interoperabilitate**

După cum s-a menționat deja în introducere, prezenta propunere se bazează pe recomandările **Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate**[35]. Acest grup, creat în iunie 2016, are scopul de a aborda provocările juridice, tehnice și operaționale pe care le presupun opțiunile disponibile pentru realizarea interoperabilității între sistemele centrale ale UE în materie de frontiere și securitate. Grupul a adoptat o perspectivă amplă și cuprinzătoare privind arhitectura de gestionare a datelor în contextul gestionării frontierelor și al asigurării respectării legii, ținând seama și de rolurile, responsabilitățile și sistemele relevante ale autorităților vamale.

Din grup au făcut parte experți din statele membre și țările Schengen asociate, precum și din agențiile europene eu-LISA, Europol, Biroul European de Sprijin pentru Azil, Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă și Agenția pentru Drepturi Fundamentale a Uniunii Europene. Au participat la acest grup, în calitate de membri cu drepturi depline, coordonatorul UE pentru lupta împotriva terorismului și Autoritatea Europeană pentru Protecția Datelor și, în calitate de observatori, reprezentanți ai Secretariatului Comisiei pentru libertăți civile, justiție și afaceri interne a Parlamentului European și ai Secretariatului General al Consiliului.

În **Raportul final întocmit de grupul de experți la nivel înalt**, publicat în mai 2017[36], se subliniază necesitatea adoptării de măsuri prin care să se soluționeze o serie de deficiențe structurale identificate în Comunicarea din aprilie 2016. Acest raport cuprinde o serie de recomandări menite să consolideze și să dezvolte sistemele de informații ale UE și interoperabilitatea acestora. Grupul a concluzionat că este **necesară și posibilă din punct de vedere tehnic crearea unui portal european de căutare, a unui serviciu comun de comparare a datelor biometrice și a unui registru comun de date de identitate ca soluții pentru interoperabilitate** și că acestea pot, în principiu, să ofere câștiguri operaționale și, totodată, să fie instituite în conformitate cu cerințele în materie de protecție a datelor. De asemenea, grupul a recomandat să se ia în considerare și posibilitatea unei abordări în două etape în ceea ce privește accesul în scopul asigurării respectării legii, pe baza unei funcționalități de marcare vizuală a rezultatelor pozitive (*hit-flagging*).

Prezentul proiect de regulament răspunde, printre altele, recomandărilor grupului de experți la nivel înalt referitoare la calitatea datelor, formatul universal pentru mesaje (UMF) și înființarea unui depozit de date [prezentat aici ca registrul central de raportare și statistici (CRRS)].

A patra componentă necesară pentru asigurarea interoperabilității propusă în prezentul proiect de regulament (detectorul de identități multiple) nu se numără printre elementele identificate de către grupul de experți la nivel înalt, dar a apărut în cursul unei analize tehnice suplimentare și al unei evaluări a proporționalității efectuate de Comisie.

---

[35] Decizia Comisiei din 17 iunie 2016 de instituire a Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate – 2016/C 257/03.

[36] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

- **Studii tehnice**

Pentru a sprijini procesul de pregătire a propunerii s-au comandat trei studii. În urma contractului semnat cu Comisia, Unisys a publicat un raport privind un studiu de fezabilitate referitor la portalul european de căutare. Agenția eu-LISA a comandat firmei Gartner (în colaborare cu Unisys) un raport tehnic privind sprijinirea dezvoltării serviciului comun de comparare a datelor biometrice. PWC a prezentat Comisiei un raport tehnic privind un registru comun de date de identitate.

- **Evaluarea impactului**

Prezenta propunere este susținută de o evaluare a impactului, astfel cum a fost prezentată în documentul de lucru al serviciilor Comisiei SWD(2017) 473, care însoțește propunerea.

În cadrul reuniunii sale din 6 decembrie 2017, Comitetul de analiză a reglementării a examinat proiectul de evaluare a impactului și, la 8 decembrie, a emis un aviz în care precizează că evaluarea impactului trebuie ajustată pentru a se ține cont de recomandările comitetului referitoare la anumite aspecte. Acestea vizau în primul rând adoptarea, în cadrul opțiunii preferate, a unor măsuri suplimentare care să raționalizeze drepturile de acces ale utilizatorilor finali la datele existente în sistemele de informații ale UE și ilustrarea garanțiilor asociate pentru protecția datelor și a drepturilor fundamentale. Cea de a doua considerație principală consta în clarificarea integrării Sistemului de informații Schengen în opțiunea 2, inclusiv printr-o analiză a eficacității și a costurilor, pentru a facilita compararea acestei opțiuni cu opțiunea 3, care este cea preferată. Comisia a actualizat evaluarea impactului pentru a ține cont atât de aceste considerații, cât și de o serie de alte considerații formulate de comitet.

În evaluarea impactului, Comisia a analizat dacă și în ce mod poate fi atins fiecare dintre obiectivele identificate, prin utilizarea uneia sau a mai multor componente tehnice identificate de grupul de experți la nivel înalt și printr-o analiză în consecință. Acolo unde a fost nevoie, Comisia a analizat subopțiunile necesare atingerii acestor obiective, respectând în același timp cadrul privind protecția datelor. Din evaluarea impactului a rezultat că:

- Pentru a îndeplini obiectivul de a asigura accesul rapid, fără sincope, sistematic și controlat al utilizatorilor autorizați la sistemele de informații relevante, ar trebui să se creeze un portal european de căutare (ESP) care să aibă la bază un serviciu comun de comparare a datelor biometrice (BMS comun), portal care să permită efectuarea de căutări în toate bazele de date.
- Pentru a îndeplini obiectivul de a facilita verificarea identității resortisanților țărilor terțe de către agenții autorizați pe teritoriul unui stat membru, ar trebui creat un registru comun de date de identitate (CIR), care să conțină setul minim de date de identificare și să aibă la bază același BMS comun.
- Pentru a îndeplini obiectivul de a detecta identitățile multiple corelate cu același set de date biometrice, cu scopul dublu de a facilita controalele de identitate pentru călătorii de bună credință și de a combate fraudele de identitate, ar trebui creat un detector de identități multiple (MID), care să conțină conexiuni între identitățile multiple din diverse sisteme.
- Pentru a îndeplini obiectivul de a facilita și simplifica accesul autorităților de aplicare a legii la sistemele de informații care nu intră în sfera asigurării respectării legii, în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor grave și a infracțiunilor de terorism, în CIR ar trebui inclusă o funcționalitate de marcare vizuală a rezultatelor pozitive („hit-flag”).

Întrucât trebuie îndeplinite toate aceste obiective, **soluția completă constă într-o combinație între ESP, CIR (cu marcarea vizuală a rezultatelor pozitive) și MID, toate acestea având la bază BMS comun**.

Cel mai mare impact pozitiv va fi îmbunătățirea gestionării frontierelor și sporirea securității interne în cadrul Uniunii Europene. Noile componente vor raționaliza și accelera accesul autorităților naționale la informațiile necesare și identificarea resortisanților țărilor terțe și le vor permite autorităților să facă conexiuni încrucișate între informațiile existente necesare privind persoanele fizice în timpul verificărilor la frontieră, în vederea prelucrării cererilor de viză sau de azil, precum și pentru activitatea polițienească. Acest lucru va permite accesul la informații care vor putea contribui la adoptarea unor decizii fiabile, fie că este vorba de decizii referitoare la investigarea unor infracțiuni grave și a unor acte de terorism, fie de decizii în domeniul migrației și azilului. Deși nu îi afectează în mod direct pe cetățenii UE (măsurile propuse se concentrează în primul rând pe resortisanții țărilor terțe ale căror date sunt înregistrate într-un sistem centralizat de informații al UE), se preconizează că măsurile propuse vor spori încrederea opiniei publice, garantând, prin modul în care sunt elaborate și aplicate, o mai bună securitate a cetățenilor UE.

Impactul financiar și economic imediat al propunerii se limitează la conceperea, dezvoltarea și exploatarea noilor instrumente. Costurile vor fi acoperite din bugetul UE și de autoritățile statelor membre responsabile cu exploatarea sistemelor. Impactul asupra turismului va fi pozitiv, având în vedere că măsurile propuse vor îmbunătăți securitatea Uniunii Europene și vor accelera controalele la frontiere. În mod similar, se prevede un impact pozitiv și asupra aeroporturilor, a porturilor maritime și a operatorilor de transport, în special datorită accelerării controalelor la frontieră.

- **Drepturile fundamentale**

În evaluarea impactului s-a analizat în special impactul măsurilor propuse asupra drepturilor fundamentale, mai cu seamă asupra dreptului la protecția datelor.

În conformitate cu Carta drepturilor fundamentale a UE, pe care instituțiile UE și statele membre trebuie să o respecte atunci când pun în aplicare legislația UE [articolul 51 alineatul (1) din Cartă], oportunitățile oferite de interoperabilitate ca măsură de consolidare a securității și de protejare a frontierelor externe trebuie să fie contrabalansate de obligația de a se asigura că eventualele atingeri care ar putea fi aduse drepturilor fundamentale ca urmare a noului context de interoperabilitate 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 de interoperabilitate propuse sunt componente complementare sistemelor existente. Din această perspectivă, ele nu vor modifica echilibrul deja asigurat de fiecare dintre sistemele centrale existente în ceea ce privește impactul lor pozitiv asupra drepturilor fundamentale.

Cu toate acestea, interoperabilitatea are potențialul de a avea un impact suplimentar indirect asupra unei serii de drepturi fundamentale. Într-adevăr, identificarea corectă a unei persoane are un impact pozitiv asupra dreptului la respectarea vieții private, și în special a dreptului la propria identitate (articolul 7 din Cartă), deoarece poate contribui la evitarea confuziilor privind identitatea. Pe de altă parte, desfășurarea de controale bazate pe date biometrice poate fi percepută ca fiind în contradicție cu dreptul la demnitate (în special, în cazul în care aceste controale sunt percepute ca fiind umilitoare) (articolul 1). Cu toate acestea, în cadrul unui sondaj[37] realizat de Agenția pentru

[37] Raportul Agenției pentru Drepturi Fundamentale a UE intitulat *FRA survey in the framework of the eu-LISA pilot on smart borders – travellers' views on and experiences of smart borders,* (Sondajul FRA în cadrul eu-LISA pilot cu privire la frontierele inteligente – opiniile călătorilor cu privire la experiențele legate de frontierele inteligente):

Drepturi Fundamentale a UE, respondenții au fost întrebați în mod direct dacă s-ar simți umiliți în cazul în care, în contextul controlului la frontieră, li s-ar preleva date biometrice. Majoritatea respondenților nu au considerat că acest lucru ar fi umilitor.

Componentele necesare pentru asigurarea interoperabilității care au fost propuse oferă prilejul adoptării de măsuri preventive specifice de consolidare a securității. Astfel, acestea pot să contribuie la protejarea dreptului la viață (articolul 2 din Cartă), ceea ce presupune, de asemenea, pentru autorități o obligație pozitivă de adoptare a unor măsuri operaționale preventive pentru a proteja o persoană a cărei viață este în pericol, în cazul în care au cunoștință sau ar fi trebuit să aibă cunoștință de existența unui risc imediat[38], precum și de a respecta interzicerea sclaviei și a muncii forțate (articolul 5). Datorită unei identificări fiabile, mai accesibile și mai ușoare, interoperabilitatea poate sprijini acțiunile de detectare a copiilor dispăruți sau a copiilor care fac obiectul traficului de persoane și poate înlesni întreprinderea unor acțiuni rapide și specifice.

O identificare mai accesibilă și mai ușoară ar putea, de asemenea, să contribuie la respectarea efectivă a dreptului de azil (articolul 18 din Cartă) și a interdicției returnării (articolul 19 din Cartă). Interoperabilitatea ar putea, de fapt, să prevină situațiile în care solicitanții de azil sunt reținuți în mod ilegal, sunt ținuți în detenție în mod ilegal sau sunt expulzați în mod nejustificat. În plus, cu ajutorul interoperabilității, fraudele de identitate vor fi mai ușor de identificat. Mai mult, va scădea necesitatea schimbului de date și informații cu țări terțe despre solicitanții de azil (în special țara de origine) pentru a stabili identitatea persoanei și pentru a obține documente de călătorie, ceea ce ar putea reprezenta un pericol pentru persoana în cauză.

- **Protecția datelor cu caracter personal**

Având în vedere datele cu caracter personal implicate, interoperabilitatea va avea în special 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 UE[39], 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[40]. Protecția datelor este strâns legată de respectarea vieții private și a celei de familie, protejată prin articolul 7 din Cartă.

În conformitate cu Regulamentul general privind protecția datelor[41], libera circulație a datelor în UE nu va fi restricționată din motive de protecție a datelor. Trebuie însă îndeplinite o serie de principii. Într-adevăr, pentru a fi legală, orice limitare a exercitării drepturilor fundamentale protejate prin Cartă trebuie să respecte următoarele criterii, stabilite la articolul 52 alineatul (1):

- trebuie să fie prevăzută de lege;

---

http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf.

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

39 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.

40 În conformitate cu articolul 52 alineatul (1) din Cartă, pot fi impuse limitări privind exercitarea dreptului la protecția datelor atât timp cât acestea sunt prevăzute prin lege, respectă substanța acestor drepturi și libertăți și, sub rezerva principiului proporționalității, sunt necesare și răspund efectiv obiectivelor de interes general recunoscute de Uniunea Europeană sau necesității protejării drepturilor și libertăților celorlalți.

41 Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

- trebuie să respecte substanța drepturilor;
- trebuie să corespundă efectiv unor obiective de interes general recunoscute de Uniune sau necesității de a proteja drepturile și libertățile altora;
- trebuie să fie necesară și
- trebuie 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”. Perioadele de păstrare a datelor (în cazul în care acestea există) sunt adecvate și limitate. 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 fiecărui sistem de informații și numai în măsura în care aceste date sunt necesare pentru îndeplinirea sarcinilor în conformitate cu aceste scopuri.

4. IMPLICAȚIILE BUGETARE

Implicațiile bugetare sunt incluse în fișa financiară anexată. Aceasta acoperă perioada rămasă din actualul cadru financiar multianual (până în 2020) și cei șapte ani din perioada următoare (2021-2027). Bugetul propus pentru 2021 și pentru anii următori este inclus cu titlu ilustrativ și nu aduce atingere următorului cadru financiar multianual.

Punerea în aplicare a acestei propuneri va necesita alocări bugetare pentru:

(1) **dezvoltarea** și integrarea de către eu-LISA a celor patru componente necesare pentru asigurarea interoperabilității și a registrului central de raportare și statistici, precum și **întreținerea și exploatarea** ulterioară a acestora;

(2) **transferul datelor** către serviciul comun de comparare a datelor biometrice (BMS comun) și către registrul comun de date de identitate (CIR). În cazul BMS comun, modelele biometrice ale datelor corespondente din cele trei sisteme care utilizează în prezent date biometrice (SIS, VIS și Eurodac) trebuie create din nou în BMS comun. În cazul CIR, trebuie asigurată migrarea datelor cu caracter personal din VIS în CIR, iar posibilele conexiuni dintre identitățile din SIS, VIS și Eurodac trebuie validate. Acest ultim proces, în special, necesită multe resurse;

(3) actualizarea de către eu-LISA a **interfeței uniforme naționale** (NUI) deja incluse în regulamentul EES, astfel încât aceasta să devină o componentă generică, în măsură să permită schimbul de mesaje între statele membre și sistemul central (sistemele centrale);

(4) **integrarea sistemelor naționale ale statelor membre** cu NUI, care va transmite mesajele schimbate cu CIR/detectorul de identități multiple prin intermediul portalului european de căutare;

(5) **formarea** privind utilizarea componentelor necesare pentru asigurarea interoperabilității de către utilizatorii finali, inclusiv cu ajutorul Agenției Uniunii Europene pentru Formare în Materie de Aplicare a Legii (CEPOL).

Componentele necesare asigurării interoperabilității sunt concepute și întreținute ca un program. Dacă portalul european de căutare (ESP) și detectorul de identități multiple sunt componente cu

totul noi, împreună cu registrul central de raportare și statistici (CRRS), BMS comun și CIR sunt componente comune care combină date existente deja păstrate (sau care urmează să fie păstrate) în sisteme noi sau deja existente, împreună cu estimările bugetare aferente.

ESP va implementa interfețele existente și cunoscute către SIS, VIS și Eurodac și, la un moment dat, se va fi extinde la noile sisteme.

ESP va fi utilizat de statele membre și agențiile care utilizează o interfață bazată pe formatul universal pentru mesaje (UMF). Această nouă interfață va trebui dezvoltată, adaptată, integrată și testată de către statele membre, eu-LISA, Europol și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă. ESP va utiliza conceptele interfeței uniforme naționale (NUI) introduse pentru EES, ceea ce va reduce eforturile de integrare.

ESP va genera costuri suplimentare pentru Europol, pentru ca interfața QUEST să poată fi utilizată pentru datele cu un nivel de protecție de bază (*basic protection level* – BPL).

Baza **BMS comun** va fi de fapt instituită odată cu crearea noului EES, deoarece acesta reprezintă de departe cel mai mare volum de date biometrice noi. Bugetul necesar a fost rezervat astfel cum se prevede în instrumentul juridic al EES. Adăugarea de noi date biometrice din SIS, VIS și Eurodac în BMS comun presupune costuri suplimentare legate în principal de migrarea datelor existente. Costurile sunt estimate la 10 milioane EUR pentru toate cele trei sisteme. Adăugarea de noi date biometrice din sistemul ECRIS-TCN propus presupune costuri suplimentare limitate, care pot fi acoperite din fondurile rezervate astfel cum se prevede în instrumentul juridic al ECRIS-TCN propus pentru înființarea unui sistem de identificare automată a amprentelor digitale ECRIS-TCN.

Registrul comun de date de identitate va fi înființat odată cu crearea viitorului EES și va fi extins ulterior, odată cu înființarea sistemului ETIAS, aflat în stadiu de propunere. Stocarea și motoarele de căutare pentru datele respective au fost incluse în bugetul rezervat, astfel cum se prevede în instrumentele juridice ale viitorului EES și ale sistemului ETIAS propus. Adăugarea de noi date biografice atât din Eurodac, cât și în sistemul ECRIS-TCN propus presupune costuri suplimentare minore, care au fost deja prevăzute în instrumentele juridice ale Eurodac și ale sistemului ECRIS-TCN propus.

Bugetul total necesar pentru o perioadă de nouă ani (2019-2027) se ridică la 424,7 milioane EUR și acoperă următoarele elemente:

(1) un buget de 225 de milioane EUR pentru eu-LISA, care acoperă costul total al dezvoltării programului, ce include cele cinci componente necesare pentru asigurarea interoperabilității (68,3 milioane EUR), costurile de întreținere din momentul în care aceste componente vor fi lansate până în 2027 (56,1 milioane EUR), un buget specific de 25 de milioane EUR pentru transferarea datelor din sistemele existente către BMS comun și costurile suplimentare pe care le presupun actualizarea NUI, rețeaua, cursurile de formare și reuniunile. Un buget specific de 18,7 milioane EUR acoperă costurile aferente modernizării și exploatării ECRIS-TCN în condiții de disponibilitate sporită începând din 2022;

(2) un buget de 136,3 milioane EUR pentru statele membre, care acoperă modificările ce trebuie aduse sistemelor lor naționale în vederea utilizării componentelor necesare pentru asigurarea interoperabilității și a interfeței NUI furnizate de eu-LISA, precum și un buget pentru formarea comunității substanțiale a utilizatorilor finali;

(3) un buget de 48,9 milioane EUR pentru Europol, care acoperă costurile de modernizare a sistemelor informatice ale Europol pentru a face față volumului de mesaje care urmează să

fie gestionate și creșterii nivelurilor de performanță[42]. Componentele necesare asigurării interoperabilității vor fi utilizate de ETIAS pentru a consulta datele Europol;

(4) un buget de 4,8 milioane EUR pentru Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă, ce va găzdui o echipă de specialiști care, în decurs de un an, vor valida conexiunile dintre identități în momentul în care detectorul de identități multiple va fi operațional;

(5) un buget de 2,0 milioane EUR pentru Agenția Uniunii Europene pentru Formare în Materie de Aplicare a Legii (CEPOL) pentru pregătirea materialelor de curs și predarea modulelor de formare pentru personalul operațional;

(6) un provizion de 7,7 milioane EUR pentru DG HOME, destinat să acopere o creștere limitată a personalului și costurile conexe în perioada de creare a diverselor componente, întrucât Comisia va trebui, la rândul său, să îndeplinească sarcini suplimentare în această perioadă și va fi responsabilă cu formatul universal pentru mesaje.

Regulamentul de instituire a Fondului pentru securitate internă (FSI) este instrumentul financiar în care s-a inclus bugetul alocat punerii în aplicare a inițiativei privind interoperabilitatea. Articolul 5 litera (b) din acest regulament prevede faptul că 791 de milioane EUR urmează să fie utilizate prin intermediul unui program pentru dezvoltarea de sisteme informatice ce au la bază sisteme informatice existente și/sau noi menite să acorde sprijin pentru gestionarea fluxurilor migratorii la frontierele externe, sub rezerva adoptării actelor legislative relevante ale Uniunii și în condițiile stabilite la articolul 15 alineatul (5). Din acești 791 de milioane EUR, 480,2 milioane EUR sunt rezervate dezvoltării EES, 210 milioane EUR, dezvoltării ETIAS și 67,9 milioane EUR, revizuirii SIS. Restul (32,9 milioane EUR) va fi realocat folosindu-se mecanismele ISF-B. Propunerea actuală solicită 32,1 milioane EUR pentru perioada rămasă din actualul cadru financiar multianual (2019/2020), care se încadrează în bugetul restant.

5. INFORMAȚII SUPLIMENTARE

- **Planuri de implementare și modalități de monitorizare, evaluare și raportare**

Agenția eu-LISA este responsabilă cu gestionarea operațională a sistemelor informatice la scară largă în spațiul de libertate, securitate și justiție (eu-LISA). Astfel, agenția este deja responsabilă cu exploatarea și îmbunătățirea tehnică și operațională a sistemelor existente și cu dezvoltarea sistemelor viitoare deja prevăzute. În temeiul prezentei propuneri de regulament, aceasta va defini configurația arhitecturii fizice a componentelor necesare pentru asigurarea interoperabilității, le va dezvolta și le va implementa și, în cele din urmă, le va găzdui. Componentele respective vor fi implementate treptat, odată cu dezvoltarea sistemelor de bază.

Comisia se va asigura că există sisteme capabile să monitorizeze dezvoltarea și funcționarea celor patru componente (portalul european de căutare, serviciul comun de comparare a datelor biometrice, registrul comun de date de identitate și detectorul de identități multiple) și a registrului central de raportare și statistici și le va evalua în funcție de principalele obiective de politică. La patru ani de la introducerea și utilizarea funcționalităților, iar apoi o dată la patru ani, eu-LISA ar trebui să prezinte Parlamentului European, Consiliului și Comisiei un raport privind funcționarea tehnică a componentelor necesare pentru asigurarea interoperabilității. În plus, la cinci ani de la

[42] Capacitatea de prelucrare a informațiilor de care dispune în prezent Europol nu este adaptată volumelor mari (în medie, 100 000 de interogări pe zi) și nici timpului de răspuns mai scurt impus de ETIAS.

introducerea și utilizarea funcționalităților, iar apoi o dată la patru ani, Comisia ar trebui să efectueze o evaluare generală a componentelor, inclusiv a impactului direct sau indirect al componentelor și a implementării lor concrete 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 trebuie să prezinte rapoartele de evaluare Parlamentului European și Consiliului.

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

Capitolul I stabilește dispozițiile generale pentru prezentul regulament și explică: principiile care stau la baza regulamentului, componentele stabilite în cadrul acestuia, obiectivele pe care urmărește să le îndeplinească interoperabilitatea, domeniul de aplicare al prezentului regulament, definițiile termenilor utilizați în prezentul regulament și principiul nediscriminării cu privire la prelucrarea datelor în temeiul prezentului regulament.

Capitolul II stabilește dispoziții privind portalul european de căutare (ESP). Acest capitol prevede instituirea ESP și definește arhitectura tehnică a acestuia, care urmează să fie realizată de către eu-LISA. Acesta precizează scopul ESP și identifică posibilii utilizatori ai ESP și modul în care aceștia urmează să îl folosească respectând drepturile de acces existente pentru fiecare dintre sistemele centrale. În acest capitol se precizează că eu-LISA va crea profiluri pentru fiecare categorie de utilizatori. Acest capitol stabilește modul în care ESP va efectua interogări în sistemele centrale și definește conținutul și formatul răspunsurilor destinate utilizatorilor. Capitolul II prevede, de asemenea, că eu-LISA păstrează înregistrările tuturor operațiunilor de prelucrare și prevede o procedură de rezervă în cazul în care ESP nu poate accesa unul sau mai multe sisteme centrale.

Capitolul III stabilește dispozițiile referitoare la serviciul comun de comparare a datelor biometrice (BMS comun). Acest capitol prevede instituirea BMS comun și definește arhitectura tehnică a acestuia, care urmează să fie realizată de către eu-LISA. Acesta precizează scopul BMS comun, stabilește datele pe care le stochează și explică relația dintre BMS comun și celelalte componente. Capitolul III prevede, de asemenea, că BMS comun nu va mai stoca datele odată ce acestea nu vor mai exista în sistemul central, iar eu-LISA va păstra înregistrările tuturor operațiunilor de prelucrare.

Capitolul IV stabilește dispoziții privind registrul comun de date de identitate (CIR). Acest capitol prevede instituirea CIR și definește arhitectura tehnică a acestuia, care urmează să fie realizată de către eu-LISA. Acesta prezintă obiectivul CIR și precizează care sunt datele care vor fi stocate și modul în care vor fi stocate, incluzând dispoziții menite să asigure calitatea datelor stocate. Acest capitol prevede că CIR va crea fișiere individuale pe baza datelor conținute în sistemele centrale și că dosarele individuale se actualizează în funcție de modificările survenite în sistemele centrale individuale. Capitolul IV specifică, de asemenea, modalitatea de funcționare a CIR în raport cu detectorul de identități multiple. Acest capitol precizează cine poate avea acces la CIR și modul în care se pot accesa datele respectându-se drepturile de acces și conține dispoziții mai specifice în funcție de obiectiv, și anume dacă accesul se face în scopul identificării sau, ca o primă etapă a abordării în două etape, în scopul accesării EES, ETIAS, VIS și Eurodac prin intermediul CIR în scopuri de asigurare a respectării legii. Capitolul IV prevede, de asemenea, că eu-LISA va păstra înregistrările tuturor operațiunilor de prelucrare referitoare la CIR.

Capitolul V stabilește dispoziții privind detectorul de identități multiple (MID). Acest capitol prevede instituirea MID și definește arhitectura tehnică a acestuia, care urmează să fie realizată de către eu-LISA. Acesta explică obiectivul MID și reglementează utilizarea MID respectându-se drepturile de acces pentru fiecare dintre sistemele centrale. Capitolul V stabilește momentul și modul în care MID va lansa căutări pentru detectarea identităților multiple, precum și modul în care vor fi prezentate rezultatele și în care li se va da curs, inclusiv, atunci când este necesar, prin verificări manuale. Capitolul V stabilește o clasificare a tipurilor de conexiuni care pot rezulta din

această căutare, în funcție de rezultatul afișat: identitate unică, identități multiple sau date de identitate partajate. Acest capitol prevede că MID va stoca datele între care s-au stabilit conexiuni păstrate în sistemele centrale, însă datele vor rămâne în cele două sau mai multe sisteme centrale individuale. Capitolul V prevede, de asemenea, că eu-LISA va păstra înregistrările tuturor operațiunilor de prelucrare referitoare la MID.

Capitolul VI prevede măsuri de susținere a interoperabilității. Acesta prevede îmbunătățirea calității datelor, crearea formatului universal pentru mesaje ca standard comun pentru schimbul de informații de asistare a interoperabilității și crearea unui registru central de raportare și statistici.

Capitolul VII se referă la protecția datelor. Acest capitol conține dispoziții care garantează prelucrarea legală și corespunzătoare a datelor în temeiul prezentului regulament, în conformitate cu dispozițiile Regulamentului (CE) nr. 45/2001. În acest capitol se explică cine va fi persoana împuternicită de către operatorul de date pentru fiecare dintre măsurile de interoperabilitate propuse în prezentul regulament și se stabilesc măsurile pe care trebuie să le adopte eu-LISA și autoritățile statelor membre pentru a garanta securitatea prelucrării datelor, confidențialitatea datelor, gestionarea corespunzătoare a incidentelor de securitate și monitorizarea respectării măsurilor prevăzute în prezentul regulament. În plus, acest capitol conține dispoziții referitoare la drepturile persoanelor vizate, inclusiv la dreptul acestora de a fi informate în legătură cu faptul că aceste date au fost stocate și prelucrate în temeiul prezentului regulament, precum și dreptul de a accesa, rectifica și șterge datele cu caracter personal care sunt stocate și prelucrate în temeiul prezentului regulament. Acest capitol stabilește principiul conform căruia datele prelucrate în temeiul prezentului regulament nu trebuie transferate sau puse la dispoziția vreunei țări terțe, organizații internaționale sau părți private, cu excepția Interpol pentru anumite scopuri specifice și cu excepția datelor primite de la Europol prin intermediul portalului european de căutare în cazul în care se aplică dispozițiile Regulamentului 2016/794 în ceea ce privește prelucrarea ulterioară a datelor. În final, capitolul conține dispoziții legate de supraveghere și de audit în ceea ce privește protecția datelor.

Capitolul VIII definește responsabilitățile eu-LISA înainte și după intrarea în vigoare a măsurilor din prezenta propunere, precum și responsabilitățile statelor membre, ale Europol și ale unității centrale a ETIAS.

Capitolul IX se referă la modificarea altor instrumente ale Uniunii. Acest capitol introduce modificări la alte instrumente juridice care sunt necesare pentru punerea în aplicare integrală a prezentei propuneri privind interoperabilitatea. Prezenta propunere include dispoziții detaliate privind modificările care trebuie aduse instrumentelor juridice care sunt în prezent texte stabile, în forma adoptată de colegiuitori: Codul Frontierelor Schengen, Regulamentul EES, Regulamentul VIS (CE), Decizia 2004/512/CE a Consiliului (Decizia VIS) și Decizia 2008/633/JAI a Consiliului (Decizia privind accesul autorităților de aplicare a legii la VIS).

Capitolul X prezintă detalii referitoare la: cerințele în materie de statistică și de raportare referitoare la datele prelucrate în temeiul prezentului regulament, măsurile tranzitorii care vor fi necesare, dispozițiile referitoare la costurile care decurg din prezentul regulament, cerințele referitoare la notificări, procedura necesară pentru ca măsurile propuse în prezentul regulament să înceapă să se aplice, dispozițiile în materie de guvernanță, inclusiv înființarea unui comitet și a unui grup consultativ, responsabilitatea eu-LISA în ceea ce privește activitățile de formare și un manual practic care să ofere recomandări cu privire la implementarea și gestionarea componentelor necesare pentru asigurarea interoperabilității, procedurile referitoare la monitorizarea și evaluarea măsurilor propuse în prezentul regulament și o dispoziție privind intrarea în vigoare a prezentului regulament.

2017/0351 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE (în materie de frontiere și vize) și de modificare a Deciziei 2004/512/CE a Consiliului, a Regulamentului (CE) nr. 767/2008, a Deciziei 2008/633/JAI a Consiliului, a Regulamentului (UE) 2016/399 și a Regulamentului (UE) 2017/2226

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16 alineatul (2), articolul 74 și articolul 77 alineatul (2) literele (a) (b) (d) și (e),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

după consultarea Autorității Europene pentru Protecția Datelor,

având în vedere avizul Comitetului Economic și Social European[43],

având în vedere avizul Comitetului Regiunilor[44],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) În comunicarea sa din 6 aprilie 2016 intitulată *„Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”*[45], Comisia a subliniat faptul că arhitectura de gestionare a datelor din Uniune în materie de gestionare a frontierelor și de securitate trebuie îmbunătățită. În urma acestei comunicări a început un proces care vizează asigurarea interoperabilității dintre sistemele de informații ale UE în materie de securitate, frontiere și gestionarea migrației, în vederea abordării deficiențelor structurale legate de aceste sisteme care împiedică autoritățile naționale să își desfășoare activitatea și în vederea accesului polițiștilor de frontieră, al autorităților vamale, al agenților de poliție și al autorităților judiciare la informațiile de care au nevoie.

(2) În Foaia de parcurs pentru a consolida schimbul de informații și gestionarea informațiilor, inclusiv soluțiile de interoperabilitate, în domeniul justiției și afacerilor interne din 6 iunie 2016[46], Consiliul a identificat diferite provocări juridice, tehnice și operaționale pe care le presupune asigurarea interoperabilității sistemelor de informații ale UE și a făcut apel la căutarea unor soluții.

(3) În Rezoluția sa din 6 iulie 2016 privind prioritățile strategice ale programului de lucru al Comisiei pentru 2017[47], Parlamentul European a solicitat Comisiei să prezinte propuneri

[43] JO C , , p. .

[44]

[45] COM(2016)205, 6.4.2016.

[46] Foaia de parcurs din 6 iunie 2016 pentru a consolida schimbul de informații și gestionarea informațiilor, inclusiv soluțiile de interoperabilitate, în domeniul justiției și afacerilor interne – 9368/1/16 REV 1.

[47] Rezoluția Parlamentului European din 6 iulie 2016 referitoare la prioritățile strategice ale programului de lucru al Comisiei pentru 2017 (2016/2773(RSP)).

pentru îmbunătățirea și dezvoltarea sistemelor de informații existente, pentru abordarea lacunelor în materie de informații și pentru asigurarea tranziției către interoperabilitate, precum și propuneri privind obligativitatea schimbului de informații la nivelul UE, însoțite de garanțiile necesare în materie de protecție a datelor.

(4) Consiliul European din 15 decembrie 2016[48] a făcut apel la continuarea asigurării interoperabilității sistemelor de informații și ale bazelor de date ale UE.

(5) În raportul său final din 11 mai 2017[49], Grupul de experți la nivel înalt pentru sistemele de informații și interoperabilitate a concluzionat că este necesar și posibil din punct de vedere tehnic să se găsească soluții practice pentru realizarea interoperabilității și că acestea pot, în principiu, să ofere câștiguri operaționale, și, totodată, să fie instituite în conformitate cu cerințele în materie de protecție a datelor.

(6) În comunicarea sa din 16 mai 2017 intitulată *Al șaptelea raport referitor la progresele înregistrate pentru realizarea unei uniuni a securității efective și reale*[50], Comisia a prezentat, în conformitate cu comunicarea sa din 6 aprilie 2016 și ținând cont de constatările și recomandările Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate, o nouă abordare privind gestionarea datelor în materie de frontiere, securitate și migrație, în care toate sistemele UE de informații privind securitatea, frontierele și gestionarea migrației urmează să fie interoperabile, cu respectarea deplină a drepturilor fundamentale.

(7) În concluziile sale din 9 iunie 2017[51] privind calea de urmat pentru îmbunătățirea schimbului de informații și asigurarea interoperabilității sistemelor de informații ale UE, Consiliul a invitat Comisia să caute în continuare soluții pentru interoperabilitate, astfel cum a propus grupul de experți la nivel înalt.

(8) Consiliul European din 23 iunie 2017[52] a subliniat necesitatea îmbunătățirii interoperabilității între bazele de date și a invitat Comisia să elaboreze, cât mai curând posibil, un proiect legislativ care să preia propunerile făcute de Grupul de experți la nivel înalt pentru sistemele de informații și interoperabilitate.

(9) Pentru îmbunătățirea gestionării frontierelor externe, pentru participarea la prevenirea și combaterea migrației neregulamentare și la asigurarea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție al Uniunii Europene, inclusiv pentru menținerea securității și a ordinii publice și pentru garantarea securității pe teritoriul statelor membre, ar trebui realizată interoperabilitatea dintre sistemele de informații ale UE, și anume [Sistemul de intrare/ieșire (EES)], Sistemul de informații privind vizele (VIS), [Sistemul european de informații și de autorizare privind călătoriile (ETIAS)], Eurodac, Sistemul de informații Schengen (SIS) și [Sistemul european de informații cu privire la cazierele judiciare pentru resortisanții țărilor terțe (ECRIS-TCN)], astfel încât aceste sisteme de informații ale UE și datele pe care le conțin să se completeze reciproc. Pentru a realiza acest lucru, trebuie instituite componentele necesare asigurării interoperabilității: un portal european de căutare (ESP), un serviciu comun de comparare a datelor biometrice (BMS comun), un registru comun de date de identitate (CIR) și un detector de identități multiple (MID).

(10) Interoperabilitatea dintre sistemele de informații ale UE ar trebui să permită completarea reciprocă pentru a facilita identificarea corectă a persoanelor, pentru a contribui la

---

48 http://www.consilium.europa.eu/ro/press/press-releases/2016/12/15/euco-conclusions-final/
49 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.
50 COM(2017) 261 final, 16.5.2017.
51 http://data.consilium.europa.eu/doc/document/ST-10151-2017-INIT/ro/pdf
52 Concluziile Consiliului European, 22-23 iunie 2017.

combaterea fraudelor de identitate, pentru a îmbunătăți și armoniza cerințele de calitate a datelor prevăzute în respectivele sisteme de informații ale UE, pentru a facilita implementarea tehnică și operațională a sistemelor de informații actuale și viitoare ale UE, pentru a consolida și simplifica garanțiile în materie de securitate și protecție a datelor prevăzute de respectivele sisteme de informații ale UE, pentru a simplifica accesul în scopul asigurării respectării legii la EES, VIS, [ETIAS] și Eurodac și pentru a îndeplini obiectivele EES, VIS, [ETIAS], Eurodac, SIS și ale [sistemului ECRIS-TCN].

(11) Componentele necesare asigurării interoperabilității ar trebui să vizeze: EES, VIS, [ETIAS], Eurodac, SIS și [sistemul ECRIS-TCN]. Acestea ar trebui, de asemenea, să vizeze datele Europol, astfel încât acestea să poată fi consultate în același timp prin intermediul acestor sisteme de informații ale UE.

(12) Componentele necesare asigurării interoperabilității ar trebui să vizeze persoanele ale căror date cu caracter personal pot fi prelucrate în sistemele de informații ale UE și de către Europol, și anume resortisanții țărilor terțe ale căror date cu caracter personal sunt prelucrate în sistemele de informații ale UE și de către Europol și cetățenii UE ale căror date cu caracter personal sunt prelucrate în SIS și de către Europol.

(13) Portalul european de căutare (ESP) ar trebui instituit pentru a facilita din punct de vedere tehnic capacitatea autorităților statelor membre și a organismelor UE de a accesa rapid, fără sincope, eficient, sistematic și controlat sistemele de informații ale UE, datele Europol și bazele de date ale Interpol de care au nevoie pentru a-și îndeplini sarcinile în conformitate cu drepturile lor de acces și de a susține obiectivele EES, VIS, [ETIAS], Eurodac, SIS, [sistemul ECRIS-TCN] și ale datelor Europol. Permițând interogarea simultană a tuturor sistemelor de informații ale UE relevante, în paralel, precum și a datelor Europol și a bazelor de date ale Interpol, ESP ar trebui să funcționeze ca un ghișeu unic sau ca un „broker de mesaje” prin care să se interogheze diverse sisteme centrale și să se extragă fără probleme informațiile necesare, cu respectarea deplină a cerințelor privind controlul accesului și protecția datelor care se aplică sistemelor de bază.

(14) Cu ajutorul bazei de date a Organizației Internaționale de Poliție Judiciară (Interpol) privind documentele de călătorie pierdute și furate (SLTD), entitățile de aplicare a legii autorizate din statele membre, inclusiv funcționarii din cadrul serviciilor de imigrare și funcționarii responsabili cu controlul la frontieră pot stabili autenticitatea unui document de călătorie. [ETIAS] interoghează banca de date SLTD și baza de date Interpol privind documentele de călătorie asociate unor notificări (TDAWN) pentru a evalua dacă o persoană care solicită o autorizație de călătorie ar putea, de exemplu, să migreze în mod neregulamentar sau ar putea constitui o amenințare la adresa securității. Portalul european de căutare centralizat (ESP) ar trebui să permită interogarea bazelor de date SLTD și TDAWN folosindu-se datele de identificare ale unei persoane. În cazul transferului de date cu caracter personal din Uniune către Interpol prin intermediul ESP, se aplică dispozițiile privind transferurile internaționale din capitolul V din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului[53] sau dispozițiile naționale de transpunere a capitolului V din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului[54]. Aceasta nu ar trebui să aducă atingere

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

[54] 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).

normelor specifice stabilite în Poziția comună 2005/69/JAI a Consiliului[55] și în Decizia 2007/533/JAI a Consiliului[56].

(15) Portalul european de căutare (ESP) ar trebui astfel dezvoltat și configurat încât, pentru interogări, să nu permită utilizarea câmpurilor de date care nu sunt legate de persoane sau de documente de călătorie sau care nu sunt prezente într-un sistem de informații al UE, în datele Europol sau în baza de date a Interpol.

(16) Pentru a asigura utilizarea rapidă și sistematică a tuturor sistemelor de informații ale UE, portalul european de căutare (ESP) ar trebui utilizat pentru efectuarea de interogări în registrul comun de date de identitate, EES, VIS, [ETIAS], Eurodac și în [sistemul ECRIS-TCN]. Cu toate acestea, conexiunea națională la diferitele sisteme de informații ale UE ar trebui menținută ca alternativă tehnică. ESP ar trebui, de asemenea, să fie utilizat de către organismele Uniunii pentru a efectua interogări în SIS central, cu respectarea drepturile lor de acces, pentru a-și îndeplini sarcinile. ESP ar trebui să fie un mijloc suplimentar de a efectua interogări în SIS central, în datele Europol și în sistemele Interpol, care să completeze interfețele dedicate deja existente.

(17) Pentru identificarea unei persoane, datele biometrice, precum amprentele digitale și imaginile faciale, sunt unice și, prin urmare, mult mai fiabile decât datele alfanumerice. Serviciul comun de comparare a datelor biometrice (BMS comun) ar trebui să fie un instrument tehnic care să consolideze și să faciliteze activitatea sistemelor de informații ale UE relevante și a celorlalte componente necesare asigurării interoperabilității. Obiectivul esențial al BMS comun ar trebui să fie facilitarea identificării unei persoane care ar putea fi înregistrată în diferite baze de date, prin compararea datelor biometrice stocate în diferite sisteme și prin folosirea unei singure componente tehnologice în loc de cinci în fiecare dintre sistemele de bază. Prin faptul că se bazează pe o componentă tehnologică unică în loc de mai multe în fiecare dintre sistemele de bază, BMS comun ar trebui să contribuie la securitate și să aducă beneficii financiare, de întreținere și operaționale. Toate sistemele automate de identificare a amprentelor digitale, inclusiv cele utilizate în prezent pentru Eurodac, VIS și SIS, utilizează modele biometrice care conțin date ce provin dintr-o extracție a unor eșantioane biometrice efective. BMS comun ar trebui să regrupeze și să stocheze toate aceste modele biometrice în același loc, facilitând comparațiile între sisteme prin utilizarea de date biometrice și permițând obținerea unor economii de scară în dezvoltarea și întreținerea sistemelor centrale ale UE.

(18) Datele biometrice reprezintă date cu caracter personal sensibile. Prezentul regulament ar trebui să stabilească baza și garanțiile privind prelucrarea unor astfel de date pentru identificarea univocă a persoanelor în cauză.

(19) Pentru a fi eficace, sistemele create prin Regulamentul (UE) 2017/2226 al Parlamentului European și al Consiliului[57], Regulamentul (CE) nr. 767/2008 al Parlamentului European și

[55] Poziția comună 2005/69/JAI a Consiliului din 24 ianuarie 2005 privind schimbul de anumite date cu Interpol (JO L 27, 29.1.2005, p. 61).

[56] Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II) (JO L 205, 7.8.2007, p. 63).

[57] Regulamentul (UE) 2017/2226 al Parlamentului European și al Consiliului din 30 noiembrie 2017 de instituire a Sistemului de intrare/ieșire (EES) pentru înregistrarea datelor de intrare și de ieșire și a datelor referitoare la refuzul intrării ale resortisanților țărilor terțe care trec frontierele externe ale statelor membre, de stabilire a condițiilor de acces la EES în scopul aplicării legii și de modificare a Convenției de punere în aplicare a Acordului Schengen și a Regulamentelor (CE) nr. 767/2008 și (UE) nr. 1077/2011 (Regulamentul EES) (JO L 327, 9.12.2017, p. 20-82).

al Consiliului[58], [Regulamentul ETIAS] pentru gestionarea frontierelor Uniunii, sistemul instituit prin [Regulamentul Eurodac] pentru identificarea solicitanților de protecție internațională și combaterea migrației neregulamentare, precum și sistemul instituit prin [Regulamentul privind sistemul ECRIS-TCN] trebuie să se bazeze pe identificarea precisă a resortisanților țărilor terțe ale căror date cu caracter personal sunt stocate în acestea.

(20) Registrul comun de date de identitate (CIR) ar trebui să faciliteze și să contribuie la identificarea corectă a persoanelor înregistrate în EES, VIS, [ETIAS], Eurodac și [sistemul ECRIS-TCN].

(21) Datele cu caracter personal stocate în aceste sisteme de informații ale UE pot face referire la aceleași persoane, dar cu identități diferite sau incomplete. Statele membre dispun de instrumente eficiente pentru identificarea cetățenilor sau a rezidenților permanenți înregistrați pe teritoriul lor, dar nu același lucru este valabil pentru resortisanții țărilor terțe. Interoperabilitatea dintre sistemele de informații ale UE ar trebui să contribuie la identificarea corectă a resortisanților țărilor terțe. Registrul comun de date de identitate (CIR) ar trebui să stocheze datele cu caracter personal privind resortisanții țărilor terțe existente în sisteme și care sunt necesare pentru a permite o identificare mai precisă a persoanelor respective, prin urmare inclusiv documentele de identitate și de călătorie și datele biometrice ale acestora, indiferent de sistemul în care au fost colectate inițial datele. În CIR ar trebui stocate doar datele cu caracter personal care sunt strict necesare pentru efectuarea unui control corect al identității. Datele cu caracter personal înregistrate în CIR nu ar trebui păstrate mai mult decât este strict necesar pentru îndeplinirea scopurilor pentru care au fost constituite sistemele de bază și trebuie șterse în mod automat atunci când datele sunt șterse din sistemele de bază, respectându-se separarea lor logică.

(22) Noua operațiune de prelucrare, care constă în stocarea acestor date în registrul comun de date de identitate (CIR) și nu în fiecare dintre sistemele separate, este necesară pentru a spori precizia identificării, care este posibilă datorită comparării și corelării automate a acestor date. Faptul că identitatea și datele biometrice ale resortisanților țărilor terțe sunt stocate în CIR nu ar trebui să împiedice în niciun fel prelucrarea datelor în sensul regulamentelor privind EES, Eurodac, VIS, ETIAS, Eurodac sau sistemul ECRIS-TCN, întrucât CIR ar urma să fie o componentă comună nouă a acestor sisteme de bază.

(23) În această privință, este necesară crearea unui dosar individual în registrul comun de date de identitate (CIR) pentru fiecare persoană înregistrată în EES, VIS, ETIAS, Eurodac sau în sistemul ECRIS-TCN, pentru realizarea obiectivului de identificare corectă a resortisanților țărilor terțe în spațiul Schengen și pentru sprijinirea detectorului de identități multiple atât pentru facilitarea controalelor de identitate pentru călătorii de bună credință, cât și pentru combaterea fraudelor de identitate. Dosarul individual ar trebui să stocheze într-un singur loc toate identitățile posibile ale unei persoane între care s-au stabilit conexiuni și să le pună la dispoziția utilizatorilor finali autorizați în mod corespunzător.

(24) Registrul comun de date de identitate (CIR) ar trebui, așadar, să susțină funcționarea detectorului de identități multiple și să faciliteze și să eficientizeze accesul autorităților de aplicare a legii la sistemele de informații ale UE care nu sunt create exclusiv în scopul prevenirii, investigării, detectării sau urmăririi penale a infracțiunilor grave.

(25) Registrul comun de date de identitate (CIR) ar trebui să prevadă un sistem comun care să conțină datele de identitate și datele biometrice ale resortisanților țărilor terțe care sunt înregistrate în EES, VIS, [ETIAS], Eurodac și în [sistemul ECRIS-TCN], care va servi drept

[58] Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS) (JO L 218, 13.8.2008, p. 60).

componentă comună acestor sisteme pentru stocarea datelor respective și în care se vor putea efectua interogări.

(26) Toate înregistrările din registrul comun de date de identitate (CIR) ar trebui separate în mod logic prin atribuirea automată a unei etichete distinctive care să lege fiecare înregistrare de sistemul sistemului de bază care deține respectiva înregistrare. Sistemul de control al accesului la CIR ar trebui să utilizeze aceste etichete pentru a permite sau nu accesul la înregistrarea respectivă.

(27) Pentru a asigura identificarea corectă a unei persoane, autoritățile competente ale statului membru, în scopul prevenirii și combaterii migrației neregulamentare, și autoritățile competente în sensul articolului 3 alineatul (7) din Directiva 2016/680 ar trebui să fie autorizate să efectueze interogări în CIR cu datele biometrice ale persoanei respective luate în cursul unui control al identității.

(28) În cazul în care datele biometrice ale persoanei respective nu pot fi utilizate sau în cazul în care, în urma interogării datelor respective, nu se obține niciun răspuns, interogarea ar trebui efectuată cu datele de identitate ale persoanei respective în combinație cu datele din documentul de călătorie. În cazul în care din interogare reiese că datele referitoare la persoana respectivă sunt înregistrate în registrul comun de date de identitate (CIR), autoritățile statelor membre ar trebui să aibă acces să consulte datele de identitate ale persoanei respective stocate în CIR, fără a furniza vreun indiciu cu privire la sistemul de informații al UE de care aparțin datele.

(29) Statele membre ar trebui să adopte măsuri legislative naționale prin care să desemneze autoritățile competente care vor efectua controale de identitate folosind registrul comun de date de identitate (CIR) și prin care să stabilească procedurile, condițiile și criteriile care trebuie respectate pentru efectuarea acestor controale, în conformitate cu principiul proporționalității. Mai precis, competența de a colecta date biometrice în cursul unui control al identității unei persoane aflate în fața unui reprezentant al acestor autorități ar trebui să fie prevăzută de dispozițiile legislative naționale.

(30) Prezentul regulament ar trebui, de asemenea, să prevadă o nouă soluție pentru simplificarea accesului autorităților de aplicare a legii desemnate de statele membre și al Europol și la alte tipuri de date din EES, VIS, [ETIAS] sau Eurodac în afară de datele de identitate. Datele, inclusiv alte tipuri de date decât datele de identitate cuprinse în aceste sisteme, pot fi necesare pentru prevenirea, detectarea, investigarea și urmărirea penală a infracțiunilor de terorism sau a infracțiunilor grave într-un anumit caz.

(31) Accesul deplin la datele conținute în sistemele de informații ale UE necesare în scopul prevenirii, depistării și investigării infracțiunilor cu caracter terorist sau a altor infracțiuni grave, în afara datelor de identitate relevante din registrul comun de date de identitate (CIR) obținute prin utilizarea datelor biometrice ale persoanei respective recoltate în cursul unui control al identității, ar trebui să fie în continuare reglementat de dispozițiile din respectivele instrumente juridice. Nici autoritățile de aplicare a legii desemnate, nici Europol nu știu dinainte care dintre sistemele de informații ale UE cuprinde date referitoare la persoanele care fac obiectul unei interogări. Acest lucru duce la întârzieri și deficiențe în desfășurarea sarcinilor. Utilizatorul final autorizat de autoritatea desemnată ar trebui să aibă posibilitatea să vadă în care dintre sistemele de informații ale UE sunt înregistrate datele corespunzătoare interogării. Sistemul în cauză va fi, prin urmare, marcat după verificarea automată a prezenței unor rezultate pozitive în sistem (marcajul vizual al rezultatelor pozitive („hit-flag”).

(32) Înregistrările interogărilor efectuate în registrul comun de date de identitate ar trebui să indice scopul acestora. În cazul în care o astfel de interogare a fost efectuată utilizându-se o

abordare în două etape de consultare a datelor, înregistrările ar trebui să includă o trimitere la dosarul național al investigației sau al cazului, indicând, prin urmare, că o astfel de interogare a fost efectuată în scopul prevenirii, depistării și investigării unor infracțiuni de terorism sau a altor infracțiuni grave.

(33) Efectuarea unei interogări în registrul comun de date de identitate (CIR) de către autoritățile desemnate dintr-un stat membru și de către Europol pentru a obține un răspuns care constă în notificarea, printr-un marcaj vizual, a existenței unor rezultate pozitive în care să se indice dacă datele sunt înregistrate în EES, VIS, [ETIAS] sau în Eurodac necesită prelucrarea automată a datelor cu caracter personal. Notificarea printr-un marcaj vizual a existenței unor rezultate pozitive nu va dezvălui datele cu caracter personal ale persoanei vizate, ci va arăta doar dacă anumite date referitoare la persoana respectivă sunt păstrate în vreunul dintre sisteme. Utilizatorul final autorizat nu va lua nicio decizie în defavoarea persoanei în cauză bazându-se exclusiv pe existența unei notificări privind un rezultat pozitiv. Prin urmare, accesul utilizatorului final la o notificare printr-un marcaj vizual a existenței unor rezultate pozitive va presupune o ingerință foarte limitată în dreptul persoanei vizate la protecția datelor cu caracter personal, însă, pentru o mai mare eficacitate, va trebui ca autoritatea desemnată și Europol să fie autorizate să solicite acces la datele cu caracter personal direct în sistemul care a fost identificat ca deținător al rezultatului pozitiv.

(34) Consultarea datelor în două etape este deosebit de importantă în cazurile în care suspecții, autorii sau victimele unei infracțiuni de terorism sau ale unei alte infracțiuni grave sunt necunoscuți. În aceste cazuri, registrul comun de date de identitate (CIR) ar trebui să permită identificarea sistemului de informații care conține date referitoare la persoana respectivă printr-o singură căutare. Prin introducerea obligației de utilizare, în aceste cazuri, a unei noi abordări privind accesul în scopul asigurării respectării legii la date, accesul la datele cu caracter personal stocate în EES, VIS, [ETIAS] și Eurodac ar trebui să aibă loc fără a fi necesară o căutare prealabilă în bazele de date naționale ori o căutare prealabilă în sistemele de identificare automată a amprentelor digitale ale altor state membre, în temeiul Deciziei 2008/615/JAI. Principiul căutării prealabile limitează într-adevăr posibilitatea autorităților statelor membre de a consulta sistemele în scopuri justificate de asigurare a respectării legii, iar acest lucru ar putea duce la situații în care se ratează ocazia de a scoate la lumină informațiile necesare. Obligația de a căuta în prealabil în bazele de date naționale și de a lansa o căutare prealabilă în sistemul de identificare automată a amprentelor digitale al altor state membre în temeiul Deciziei 2008/615/JAI ar trebui să nu se mai aplice doar din momentul în care va deveni operațională garanția alternativă a abordării în două etape a accesului în scopul asigurării respectării legii prin intermediul CIR.

(35) Ar trebui instituit detectorul de identități multiple (MID) pentru a sprijini funcționarea registrului comun de date de identitate și pentru a susține realizarea obiectivelor EES, VIS, [ETIAS], Eurodac, SIS și ale [sistemului ECRIS-TCN]. Pentru a fi eficace în ceea ce privește îndeplinirea obiectivelor lor respective, toate aceste sisteme de informații ale UE necesită identificarea precisă a persoanelor ale căror date cu caracter personal sunt stocate în ele.

(36) Posibilitatea îndeplinirii obiectivelor sistemelor de informații ale UE este subminată de faptul că, în prezent, autoritățile care utilizează aceste sisteme nu au posibilitatea de a efectua verificări suficient de fiabile cu privire la identitatea resortisanților țărilor terțe ale căror date sunt înregistrate în diverse sisteme. Această imposibilitate derivă din faptul că datele de identitate stocate într-un anumit sistem pot fi frauduloase, incorecte sau incomplete și că în prezent nu există nicio posibilitate de detectare a datelor de identitate frauduloase, incorecte sau incomplete prin comparație cu datele stocate într-un alt sistem. Pentru a

remedia această situație, este necesar ca la nivelul Uniunii să existe un instrument tehnic care să permită identificarea precisă a resortisanților țărilor terțe în aceste scopuri.

(37) *Detectorul de identități multiple (MID)* ar trebui să creeze și să stocheze conexiunile dintre datele stocate în diferitele sisteme de informații ale UE în vederea detectării identităților multiple, cu scopul dublu de a facilita controalele de identitate pentru călătorii de bună credință și, în același timp, de a combate fraudele de identitate. MID ar trebui să conțină exclusiv conexiunile dintre persoanele prezente în mai multe sisteme centrale de informații, care se limitează în mod strict la datele necesare pentru a verifica dacă o persoană este înregistrată în mod legal sau ilegal cu mai multe identități biografice diferite în sisteme diferite sau pentru a clarifica dacă două persoane cu date biografice similare nu sunt, de fapt, aceeași persoană. Prelucrarea datelor prin intermediul portalului european de căutare (ESP) și al serviciului comun de comparare a datelor biometrice (BMS comun) în vederea stabilirii de conexiuni între dosarele individuale din diverse sisteme ar trebui menținută la un nivel minim absolut și, prin urmare, se limitează la o detectare a identităților multiple atunci când se adaugă date noi în unul dintre sistemele de informații incluse în registrul comun de date de identitate și în SIS. MID ar trebui să includă garanții împotriva unor eventuale cazuri de discriminare sau a unor decizii nefavorabile care vizează persoane cu identități multiple legale.

(38) Prezentul regulament prevede noi operațiuni de prelucrare a datelor care vizează identificarea corectă a persoanelor în cauză. Aceasta constituie o ingerință în drepturile lor fundamentale, astfel cum sunt protejate prin articolele 7 și 8 din Carta drepturilor fundamentale. Întrucât implementarea efectivă a sistemelor de informații ale UE depinde de identificarea corectă a persoanelor în cauză, o astfel de ingerință este justificată prin invocarea acelorași obiective ca și cele care stau la baza instituirii fiecăruia dintre aceste sisteme: gestionarea eficace a frontierelor Uniunii, securitatea internă a Uniunii, punerea în aplicare eficace a politicilor Uniunii în materie de azil și vize și lupta împotriva migrației neregulamentare.

(39) Atunci când o autoritate națională sau un organism al UE creează noi înregistrări, portalul european de căutare (ESP) și serviciul comun de comparare a datelor biometrice (BMS comun) ar trebui să compare datele privind persoanele în registrul comun de date de identitate (CIR) și în SIS. O astfel de comparație ar trebui să fie automatizată. CIR și SIS ar trebui să utilizeze BMS comun pentru a detecta posibilele conexiuni pe baza datelor biometrice. CIR și SIS ar trebui să utilizeze ESP pentru a detecta posibilele conexiuni pe baza datelor alfanumerice. CIR și SIS ar trebui să fie în măsură să identifice datele identice sau similare privind un resortisant al unei țări terțe stocate în mai multe sisteme. Dacă este cazul, ar trebui creată o conexiune care să indice că este vorba de aceeași persoană. CIR și SIS ar trebui astfel configurate încât greșelile minore de ortografie sau de transcriere să fie detectate, în așa fel încât să nu se creeze obstacole nejustificate pentru resortisantul țării terțe în cauză.

(40) Autoritatea națională sau organismul UE care a înregistrat datele respective în sistemul de informații ar trebui să confirme sau să modifice aceste conexiuni. Această autoritate ar trebui să aibă acces la datele stocate în registrul comun de date de identitate (CIR) sau în SIS, precum și în detectorul de identități multiple (MID), în scopul verificării manuale a identității.

(41) Accesul la detectorul de identități multiple (MID) al autorităților statelor membre și al organismelor UE care au acces la cel puțin un sistem de informații al UE inclus în registrul comun de date de identitate (CIR) sau la SIS ar trebui limitat la așa-numitele conexiuni roșii, în care datele conexate conțin aceleași date biometrice, dar date de identitate diferite, iar

autoritatea responsabilă cu verificarea diferitelor identități a concluzionat că acestea se referă în mod ilegal la aceeași persoană sau în care datele conexate conțin date biometrice similare, iar autoritatea responsabilă cu verificarea diferitelor identități a concluzionat că acestea se referă în mod ilegal la aceeași persoană. În cazul în care datele de identitate conexate nu sunt similare, ar trebui să se creeze o conexiune galbenă și să se efectueze o verificare manuală pentru confirmarea conexiunii sau schimbarea culorii în consecință.

(42) Verificarea manuală a identităților multiple ar trebui asigurată de către autoritatea care a creat sau actualizat datele care au generat un rezultat pozitiv, în urma căruia s-a stabilit o conexiune cu date înregistrate deja în alt sistem de informații al UE. Autoritatea responsabilă cu verificarea identităților multiple ar trebui să evalueze dacă există mai multe identități legale sau ilegale. Această evaluare ar trebui efectuată, dacă este posibil, în prezența resortisantului dintr-o țară terță, solicitându-se, dacă este necesar, clarificări sau informații suplimentare. Această evaluare ar trebui efectuată fără întârziere, în conformitate cu cerințele legale privind exactitatea informațiilor în temeiul legislației Uniunii și a legislației naționale.

(43) Pentru conexiunile obținute în ceea ce privește Sistemul de informații Schengen (SIS), referitoare la semnalări privind persoane căutate pentru a fi arestate ori în vederea predării sau a extrădării, privind persoane dispărute sau vulnerabile, privind persoane căutate în vederea participării la o procedură judiciară, privind persoane vizate pentru controale discrete sau controale specifice sau privind persoane căutate necunoscute, autoritatea responsabilă cu verificarea identităților multiple ar trebui să fie biroul SIRENE din statul membru care a creat semnalarea. Într-adevăr, aceste categorii de semnalări SIS sunt sensibile și nu ar trebui neapărat să facă obiectul unui schimb cu autoritățile care au creat sau actualizat datele din unul dintre celelalte sisteme de informații ale UE. Crearea unei conexiuni cu datele din SIS nu ar trebui să aducă atingere măsurilor care urmează să fie adoptate în conformitate cu [Regulamentele SIS].

(44) Agenția eu-LISA ar trebui să instituie mecanisme automatizate de control al calității datelor și indicatori comuni ai calității datelor. În plus, ar trebui să fie responsabilă cu dezvoltarea unei capacități centrale de monitorizare pentru calitatea datelor și să prezinte în mod regulat rapoarte de analiză a datelor în vederea îmbunătățirii controlului în ceea ce privește implementarea și utilizarea sistemelor de informații ale UE de către statele membre. Indicatorii comuni de calitate ar trebui să includă standarde minime de calitate pentru stocarea datelor în sistemele de informații ale UE sau în componentele necesare asigurării interoperabilității. Scopul standardelor de calitate privind datele ar trebui să fie, pentru sistemele de informații ale UE sau pentru componentele necesare asigurării interoperabilității, acela de a identifica în mod automat datele care par a fi incorecte sau inconsecvente, astfel încât statul membru din care provin să fie în măsură să le verifice și să ia măsurile necesare pentru a le corecta.

(45) Comisia ar trebui să evalueze rapoartele privind calitatea întocmite de eu-LISA și, după caz, ar trebui să formuleze recomandări adresate statelor membre. Statele membre ar trebui să fie responsabile cu pregătirea unui plan de acțiune care să descrie măsurile care vizează remedierea eventualelor deficiențe în ceea ce privește calitatea datelor și ar trebui să prezinte periodic progresele înregistrate.

(46) Formatul universal de mesaje (UMF) ar trebui să stabilească un standard pentru schimburile de informații transfrontaliere structurate între sistemele de informații, autoritățile și/sau organizațiile din domeniul justiției și afacerilor interne. UMF ar trebui să definească un vocabular comun și structuri logice pentru informațiile care fac frecvent obiectul

schimburilor, cu scopul de a facilita interoperabilitatea, permițând crearea și citirea conținutului în mod coerent și cu asigurarea echivalenței semantice.

(47) Ar trebui înființat un registru central de raportare și statistici (CRRS) care să genereze date statistice între sisteme și rapoarte analitice în scopuri strategice, operaționale și de asigurare a calității datelor. Agenția eu-LISA ar trebui să instituie, să implementeze și să găzduiască CRRS în localurile sale tehnice care conțin date statistice anonime din sistemele menționate mai sus, din registrul comun de date de identitate, din detectorul de identități multiple și din serviciul comun de comparare a datelor biometrice. Datele conținute în CRRS nu ar trebui să permită identificarea persoanelor. Agenția eu-LISA ar trebui să anonimizeze datele și ar trebui să înregistreze aceste date anonime în CRRS. Procesul de anonimizare a datelor nu ar trebui să fie automatizat, iar personalul eu-LISA nu ar trebui să aibă acces direct la datele cu caracter personal stocate în sistemele de informații ale UE sau în componentele necesare asigurării interoperabilității.

(48) Regulamentul (UE) 2016/679 ar trebui să se aplice prelucrării datelor cu caracter personal efectuate în temeiul prezentului regulament de către autoritățile naționale, cu excepția cazului în care această prelucrare este efectuată de către autoritățile desemnate sau de către punctele centrale de acces din statele membre în scopul prevenirii, depistării sau investigării infracțiunilor de terorism sau a altor infracțiuni grave, caz în care ar trebui să se aplice Directiva (UE) 2016/680 a Parlamentului European și a Consiliului.

(49) Dispozițiile specifice privind protecția datelor din [Regulamentul EES], Regulamentul (CE) nr. 767/2008 [Regulamentul ETIAS] și [Regulamentul SIS în domeniul verificărilor la frontiere] ar trebui să se aplice prelucrării datelor cu caracter personal în cadrul sistemelor respective.

(50) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului[59] ar trebui să se aplice în cazul prelucrării datelor cu caracter personal de către eu-LISA și de către alte instituții și organisme ale Uniunii atunci când își exercită responsabilitățile care le revin în temeiul prezentului regulament, fără a aduce atingere dispozițiilor Regulamentului (UE) 2016/794, care ar trebui să se aplice prelucrării datelor cu caracter personal de către Europol.

(51) Autoritățile naționale de supraveghere instituite în conformitate cu [Regulamentul (UE) 2016/679] ar trebui să monitorizeze legalitatea prelucrării datelor cu caracter personal de către statele membre, iar Autoritatea Europeană pentru Protecția Datelor, instituită prin Regulamentul (CE) nr. 45/2001, ar trebui să monitorizeze activitățile instituțiilor și organelor Uniunii în ceea ce privește prelucrarea datelor cu caracter personal. Autoritatea Europeană pentru Protecția Datelor și autoritățile de supraveghere ar trebui să coopereze între ele în cadrul activităților de monitorizare a prelucrării datelor de către componentele necesare asigurării interoperabilității.

(52) „(...) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 și a emis un aviz la ...”

(53) În ceea ce privește confidențialitatea, funcționarilor sau altor agenți care sunt angajați și își desfășoară activitatea în legătură cu SIS ar trebui să li se aplice dispozițiile corespunzătoare din Statutul funcționarilor Uniunii Europene și din Regimul aplicabil celorlalți agenți ai Uniunii Europene.

(54) Atât statele membre, cât și eu-LISA ar trebui să dispună de planuri de securitate pentru a facilita îndeplinirea obligațiilor privind securitatea și ar trebui să coopereze între ele pentru a

[59] Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

aborda chestiunile legate de securitate. Agenția eu-LISA ar trebui, de asemenea, să se asigure că sunt valorificate permanent cele mai recente evoluții tehnologice pentru a asigura integritatea datelor în ceea ce privește dezvoltarea, proiectarea și gestionarea componentelor necesare asigurării interoperabilității.

(55) Implementarea componentelor necesare asigurării interoperabilității prevăzute în prezentul regulament vor avea un impact asupra modului în care se efectuează controalele la punctele de trecere a frontierei. Aceste impacturi vor fi rezultatul aplicării coroborate a normelor în vigoare prevăzute de Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului[60] și a normelor privind interoperabilitatea prevăzute în prezentul regulament.

(56) Ca o consecință a acestei aplicări combinate a normelor, portalul european de căutare (ESP) ar trebui să constituie principalul punct de acces pentru consultarea sistematică obligatorie a bazelor de date pentru resortisanții țărilor terțe la punctele de trecere a frontierei, astfel cum este prevăzută în Codul frontierelor Schengen. În plus, polițiștii de frontieră care evaluează dacă o persoană îndeplinește condițiile de intrare definite în Codul frontierelor Schengen ar trebui să țină cont de datele de identitate care au condus la încadrarea unei conexiuni în detectorul de identități multiple (MID) în categoria conexiunilor roșii. Cu toate acestea, prezența unui conexiuni roșii nu ar trebui să constituie în sine un motiv de refuz al intrării; așadar, motivele de refuz al intrării prevăzute în Codul frontierelor Schengen nu ar trebui modificate.

(57) Manualul practic pentru polițiștii de frontieră va trebui actualizat, astfel încât aceste precizări să fie explicite.

(58) Cu toate acestea, este necesară modificarea Regulamentului (UE) 2016/399 pentru a se adăuga obligația ca, pentru a nu prelungi timpul de așteptare la controalele din prima linie, polițistul de frontieră să supună resortisantul unei țări terțe unui control în linia a doua, în cazul în care, în urma consultării detectorului de identități multiple (MID) prin intermediul portalului european de căutare (ESP), reiese că există o conexiune galbenă sau roșie.

(59) În cazul în care, în urma interogării detectorului de identități multiple (MID) prin intermediul portalului european de căutare (ESP), se identifică o conexiune galbenă sau roșie, polițistul de frontieră din a doua linie ar trebui să consulte registrul comun de date de identitate sau Sistemul de informații Schengen, sau ambele, pentru a verifica informațiile privind persoana controlată, pentru a verifica manual diferitele sale identități și pentru a adapta culoarea conexiunii, dacă este necesar.

(60) În vederea sprijinirii întocmirii de statistici și rapoarte, este necesar ca personalul autorizat al autorităților competente, al instituțiilor și al organismelor identificate în prezentul regulament să aibă acces la anumite date referitoare la anumite componente necesare asigurării interoperabilității, dar nu și la date care ar permite identificarea persoanelor.

(61) Pentru ca autoritățile competente și organismele UE să se poată adapta noilor cerințe privind utilizarea portalului european de căutare (ESP), este necesar să se prevadă o perioadă de tranziție. În mod similar, pentru a se asigura coerența și funcționarea optimă a detectorului de identități multiple (MID), ar trebui stabilite măsuri tranzitorii pentru punerea în funcțiune a acestuia.

(62) Costurile pentru dezvoltarea componentelor necesare asigurării interoperabilității prevăzute de cadrul financiar multianual actual sunt mai mici decât suma rămasă din bugetul alocat frontierelor inteligente în Regulamentul (UE) nr. 515/2014 al Parlamentului European și al

[60] Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului din 9 martie 2016 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen), JO L 77, 23.3.2016, p. 1.

Consiliului[61]. Prin urmare, în temeiul articolului 5 alineatul (5) litera (b) din Regulamentul (UE) nr. 515/2014, prezentul regulament ar trebui să realoce suma destinată în prezent dezvoltării de sisteme informatice care sprijină gestionarea fluxurilor migratorii la frontierele externe.

(63) Pentru a completa anumite aspecte tehnice detaliate ale prezentului regulament, competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene ar trebui să fie delegată Comisiei în ceea ce privește profilurile utilizatorilor portalului european de căutare (ESP) și conținutul și formatul rezultatelor afișate de ESP. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional privind o mai bună legiferare din 13 aprilie 2016[62]. Mai precis, pentru a se asigura participarea într-o măsură egală a acestora la elaborarea actelor delegate, Parlamentul European și Consiliul ar trebui să primească toate documentele în același timp cu experții din statele membre, iar experții acestor instituții ar trebui să aibă în mod sistematic acces la reuniunile grupurilor de experți ale Comisiei însărcinate cu elaborarea actelor delegate.

(64) Pentru a asigura condiții uniforme pentru punerea în aplicare a prezentului regulament, Comisiei ar trebui să i se delege competențe de executare în vederea adoptării unor norme detaliate privind: mecanismele și procedurile automatizate de control al calității datelor și indicatorii aferenți, dezvoltarea standardului UMF, procedurile de identificare a cazurilor de similitudine a identităților; funcționarea registrului central de raportare și statistici și procedura de cooperare în cazul unor incidente de securitate. Aceste competențe ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului[63].

(65) Regulamentul 2016/794 se aplică în cazul oricărei prelucrări de date Europol în sensul prezentului regulament.

(66) Prezentul regulament nu aduce atingere aplicării Directivei 2004/38/CE.

(67) Prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen.

(68) 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. Deoarece prezentul regulament constituie o dezvoltare a acquis-ului Schengen, Danemarca decide, în conformitate cu articolul 4 din protocolul respectiv, în termen de șase luni de la adoptarea prezentului regulament, dacă îl va pune în aplicare în legislația sa națională.

(69) Prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen la care Regatul Unit nu participă, în conformitate cu Decizia 2000/365/CE a Consiliului[64]; prin urmare, Regatul Unit nu participă la adoptarea prezentului regulament, nu are obligații în temeiul acestuia și nu face obiectul aplicării sale.

---

[61] Regulamentul (UE) nr. 515/2014 al Parlamentului European și al Consiliului din 16 aprilie 2014 de instituire, în cadrul Fondului pentru securitate internă, a instrumentului de sprijin financiar pentru frontiere externe și vize și de abrogare a Deciziei nr. 574/2007/CE (JO L 150, 20.5.2014, p. 143).

[62] http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32016Q0512(01)&from=EN

[63] 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).

[64] Decizia 2000/365/CE a Consiliului din 29 mai 2000 privind solicitarea Regatului Unit al Marii Britanii și Irlandei de Nord de a participa la unele dintre dispozițiile acquis-ului Schengen (JO L 131, 1.6.2000, p. 43).

(70) Prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen la care Irlanda nu participă, în conformitate cu Decizia 2002/192/CE a Consiliului[65]; Prin urmare, Irlanda nu participă la adoptarea prezentului regulament, nu are obligații în temeiul acestuia și nu face obiectul aplicării sale.

(71) În ceea ce privește Islanda și Norvegia, prezentul regulament reprezintă o dezvoltare a dispozițiilor acquis-ului Schengen, în sensul Acordului încheiat între Consiliul Uniunii Europene și Republica Islanda și Regatul Norvegiei privind asocierea acestora din urmă la transpunerea, punerea în aplicare și dezvoltarea acquis-ului Schengen[66], care intră sub incidența articolului 1 punctele A, B și G din Decizia 1999/437/CE a Consiliului din 17 mai 1999 privind anumite norme de aplicare a respectivului acord[67].

(72) În ceea ce privește Elveția, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen, în sensul Acordului dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană cu privire la asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen[68], care se încadrează în domeniul menționat la articolul 1 punctele A, B și G din Decizia 1999/437/CE, coroborat cu articolul 3 din Decizia 2008/146/CE a Consiliului[69].

(73) În ceea ce privește Liechtenstein, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen, în sensul Protocolului între Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein cu privire la aderarea Principatului Liechtenstein la Acordul între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, asigurarea respectării și dezvoltarea acquis-ului Schengen[70], care se încadrează în domeniul menționat la articolul 1 punctele A, B și G din Decizia 1999/437/CE, coroborat cu articolul 3 din Decizia 2011/350/UE a Consiliului[71].

(74) În ceea ce privește Ciprul, dispozițiile referitoare la SIS și la VIS reprezintă dispoziții bazate pe acquis-ul Schengen – sau care se raportează în alt mod la acesta – în sensul articolului 3 alineatul (2) din Actul de aderare din 2003.

(75) În ceea ce privește Bulgaria și România, dispozițiile referitoare la SIS și la VIS reprezintă dispoziții bazate pe acquis-ul Schengen – sau care se raportează în alt mod la acesta – în sensul articolului 4 alineatul (2) din Actul de aderare din 2005, coroborat cu Decizia 2010/365/UE a Consiliului[72] și cu Decizia (UE) 2017/1908 a Consiliului[73].

(76) În ceea ce privește Croația, dispozițiile referitoare la SIS și la VIS reprezintă dispoziții bazate pe acquis-ul Schengen – sau care se raportează în alt mod la acesta – în sensul

---

[65] Decizia 2002/192/CE a Consiliului din 28 februarie 2002 privind solicitarea Irlandei de a participa la unele dintre dispozițiile acquis-ului Schengen (JO L 64, 7.3.2002, p. 20).

[66] JO L 176, 10.7.1999, p. 36.

[67] JO L 176, 10.7.1999, p. 31.

[68] JO L 53, 27.2.2008, p. 52.

[69] JO L 53, 27.2.2008, p. 1.

[70] JO L 160, 18.6.2011, p. 21.

[71] JO L 160, 18.6.2011, p. 19.

[72] Decizia 2010/365/UE a Consiliului din 29 iunie 2010 privind aplicarea dispozițiilor acquis-ului Schengen referitoare la Sistemul de informații Schengen în Republica Bulgaria și în România (JO L 166, 1.7.2010, p. 17).

[73] Decizia (UE) 2017/1908 a Consiliului din 12 octombrie 2017 privind punerea în aplicare a anumitor dispoziții ale acquis-ului Schengen referitoare la Sistemul de informații privind vizele în Republica Bulgaria și în România (JO L 269, 19.10.2017, p. 39).

articolului 4 alineatul (2) din Actul de aderare din 2011 coroborat cu Decizia (UE) 2017/733 a Consiliului[74].

(77) Prezentul regulament respectă drepturile fundamentale și se conformează principiilor recunoscute, în special, de Carta drepturilor fundamentale a Uniunii Europene, și se aplică în conformitate cu aceste drepturi și principii.

(78) Pentru ca prezentul regulament să se încadreze în cadrul juridic existent, Regulamentul (UE) 2016/399, Regulamentul (UE) 2017/2226, Decizia 2008/633/JAI a Consiliului, Regulamentul (CE) nr. 767/2008 și Decizia 2004/512/CE a Consiliului ar trebui modificate în consecință,

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I
Dispoziții generale

Articolul 1
Obiect

1. Prezentul regulament, împreună cu [Regulamentul 2018/xx privind interoperabilitatea, cooperarea polițienească și judiciară, azilul și migrația], stabilește un cadru pentru a asigura interoperabilitatea dintre Sistemul de intrare/ieșire (EES), Sistemul de informații privind vizele (VIS), [Sistemul european de informații și de autorizare privind călătoriile (ETIAS)], Eurodac, Sistemul de informații Schengen (SIS) și [Sistemul european de informații cu privire la cazierele judiciare ale resortisanților țărilor terțe (ECRIS-TCN)], astfel încât aceste sisteme și date să se completeze reciproc.

2. Cadrul include următoarele componente de interoperabilitate:

   (a) un portal european de căutare (ESP);

   (b) un serviciu comun de comparare a datelor biometrice (BMS comun);

   (c) un registru comun de date de identitate (CIR);

   (d) un detector de identități multiple (MID).

3. Prezentul regulament cuprinde, de asemenea, dispoziții privind cerințele de calitate a datelor, formatul universal pentru mesaje (UMF) și registrul central de raportare și statistici (CRRS) și stabilește responsabilitățile statelor membre și ale Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA) în ceea ce privește conceperea și funcționarea componentelor de interoperabilitate.

4. Prezentul regulament adaptează totodată procedurile și condițiile în care autoritățile de aplicare a legii ale statelor membre și Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) au acces la Sistemul de intrare/ieșire (EES), Sistemul de informații privind vizele (VIS), [Sistemul european de informații și de autorizare privind călătoriile (ETIAS)] și Eurodac în scopul prevenirii, depistării și

[74] Decizia (UE) 2017/733 a Consiliului din 25 aprilie 2017 privind aplicarea dispozițiilor acquis-ului Schengen referitoare la Sistemul de Informații Schengen în Republica Croația (JO L 108, 26.4.2017, p. 31).

investigării infracțiunilor de terorism sau a altor infracțiuni grave care sunt de competența lor.

Articolul 2
Obiectivele interoperabilității

1. Prin asigurarea interoperabilității, prezentul regulament are următoarele obiective:

   (a) îmbunătățirea gestionării frontierelor externe;

   (b) contribuirea la prevenirea și combaterea migrației neregulamentare;

   (c) contribuirea la asigurarea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție al Uniunii, inclusiv la menținerea siguranței publice și a ordinii publice și la garantarea securității pe teritoriul statelor membre;

   (d) îmbunătățirea punerii în aplicare a politicii comune în materie de vize și

   (e) facilitarea examinării cererilor de protecție internațională.

2. Obiectivele legate de asigurarea interoperabilității sunt realizate prin:

   (a) asigurarea identificării corecte a persoanelor;

   (b) contribuirea la combaterea fraudelor de identitate;

   (c) îmbunătățirea și armonizarea cerințelor de calitate a datelor aplicate în diferitele sisteme de informații ale UE;

   (d) facilitarea implementării tehnice și operaționale de către statele membre a sistemelor de informații actuale și viitoare ale UE;

   (e) consolidarea și simplificarea condițiilor privind securitatea și protecția datelor care guvernează diferitele sisteme de informații ale UE și sporirea uniformității acestor condiții;

   (f) raționalizarea condițiilor de acces la EES, VIS, [ETIAS] și Eurodac în scopul asigurării respectării legii;

   (g) sprijinirea realizării scopurilor pentru care au fost instituite EES, VIS, [ETIAS], Eurodac, SIS și [ECRIS-TCN].

Articolul 3
Domeniul de aplicare

1. Prezentul regulament se aplică [Sistemului de intrare/ieșire (EES)], Sistemului de informații privind vizele (VIS), [Sistemului european de informații și de autorizare privind călătoriile (ETIAS)] și Sistemului de informații Schengen (SIS).

2. Prezentul regulament se aplică persoanelor ale căror date cu caracter personal pot fi prelucrate în sistemele de informații ale UE la care se face referire la alineatul (1).

Articolul 4
Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

   (1) „frontiere externe” înseamnă frontierele externe, astfel cum sunt definite la articolul 2 punctul 2 din Regulamentul (UE) 2016/399;

(2) „verificări la frontiere” înseamnă verificările la frontiere, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (UE) 2016/399;

(3) „autoritate de frontieră” înseamnă polițistul de frontieră însărcinat, în conformitate cu dreptul intern, să efectueze verificări la frontiere;

(4) „autorități de supraveghere” înseamnă autoritatea de supraveghere instituită în conformitate cu articolul 51 alineatul (1) din Regulamentul (UE) 2016/679 și autoritatea de supraveghere instituită în conformitate cu articolul 41 alineatul (1) din Directiva (UE) 2016/680;

(5) „verificare” înseamnă procesul de comparare a unor serii de date în vederea stabilirii autenticității unei identități declarate (verificare realizată prin compararea unei mostre cu o serie de date);

(6) „identificare” înseamnă procesul de stabilire a identității unei persoane efectuându-se o căutare într-o bază de date prin compararea cu mai multe serii de date (verificare realizată prin compararea unei mostre cu serii multiple de date);

(7) „resortisant al unei țări terțe” înseamnă o persoană care nu este cetățean al Uniunii în sensul articolului 20 alineatul (1) din tratat sau un apatrid ori o persoană a cărei cetățenie este necunoscută;

(8) „date alfanumerice” înseamnă date constând în litere, cifre, caractere speciale, spații și semne de punctuație;

(9) „date de identitate” înseamnă datele prevăzute la articolul 27 alineatul (3) literele (a)-(h);

(10) „date dactiloscopice” înseamnă datele privind amprentele digitale ale unei persoane;

(11) „imagine facială” înseamnă imagini digitale ale feței;

(12) „date biometrice” înseamnă datele dactiloscopice și/sau imaginea facială;

(13) „model biometric” înseamnă o reprezentare matematică obținută prin extragerea din datele biometrice a parametrilor aferenți caracteristicilor necesare pentru efectuarea de identificări și verificări;

(14) „document de călătorie” înseamnă pașaportul sau un alt document echivalent care îi dă titularului dreptul de trecere a frontierelor externe și pe care se poate aplica o viză;

(15) „date din documentul de călătorie” înseamnă tipul și numărul documentului de călătorie, țara care l-a eliberat, data expirării perioadei de valabilitate a documentului de călătorie și codul din trei litere al țării care a eliberat documentul de călătorie;

(16) „autorizație de călătorie” înseamnă o autorizație de călătorie, astfel cum este definită la articolul 3 din [Regulamentul privind ETIAS];

(17) „viză de scurtă ședere” înseamnă o viză, astfel cum este definită la articolul 2 punctul 2 litera (a) din Regulamentul (CE) nr. 810/2009;

(18) „sisteme de informații ale UE” înseamnă sistemele informatice la scară largă gestionate de eu-LISA;

(19) „date Europol” înseamnă datele cu caracter personal furnizate Europol în scopul menționat la articolul 18 alineatul (2) litera (a) din Regulamentul (UE) 2016/794;

(20) „baze de date ale Interpol” înseamnă baza de date a Interpol privind documentele de călătorie furate și pierdute (SLTD) și baza de date a Interpol privind documentele de călătorie asociate unor notificări (TDAWN a Interpol);

(21) „concordanță” înseamnă existența unei corespondențe stabilite prin compararea a două sau mai multe ocurențe de 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;

(22) „rezultat pozitiv” înseamnă confirmarea uneia sau mai multor concordanțe;

(23) „autoritate polițienească” înseamnă „autoritate competentă”, astfel cum este definită la articolul 3 punctul 7 din Directiva 2016/680;

(24) „autorități desemnate” înseamnă autoritățile desemnate de statele membre și menționate la articolul 29 alineatul (1) din Regulamentul (UE) 2017/2226, la articolul 3 alineatul (1) din Decizia 2008/633/JAI a Consiliului, [la articolul 43 din Regulamentul privind ETIAS] și [la articolul 6 din Regulamentul privind Eurodac];

(25) „infracțiune de terorism” înseamnă o infracțiune prevăzută în dreptul național care corespunde unei infracțiuni menționate în Directiva (UE) 2017/541 sau este echivalentă cu una dintre acestea;

(26) „infracțiune gravă” înseamnă o infracțiune care corespunde unei infracțiuni prevăzute la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI sau care este echivalentă cu una dintre acestea dacă se pedepsește în dreptul intern cu închisoarea sau cu o măsură de siguranță privativă de libertate pe o perioadă maximă de cel puțin trei ani;

(27) „EES” înseamnă Sistemul de intrare/ieșire, astfel cum este menționat în Regulamentul (UE) 2017/2226;

(28) „VIS” înseamnă Sistemul de informații privind vizele, astfel cum este menționat în Regulamentul (CE) nr. 767/2008;

(29) [„ETIAS” înseamnă Sistemul european de informații și de autorizare privind călătoriile, astfel cum este menționat în Regulamentul privind ETIAS];

(30) „Eurodac” înseamnă Eurodac, astfel cum este menționat în [Regulamentul privind Eurodac];

(31) „SIS” înseamnă Sistemul de informații Schengen, astfel cum este menționat în [Regulamentul privind SIS în domeniul verificărilor la frontiere, Regulamentul privind SIS în domeniul asigurării respectării legii și Regulamentul privind SIS în domeniul returnării ilegale];

(32) [„ECRIS-TCN” înseamnă Sistemul european de informații cu privire la cazierele judiciare, în care există informații privind condamnările resortisanților țărilor terțe și ale apatrizilor, astfel cum se menționează în Regulamentul privind ECRIS-TCN)];

(33) „ESP” înseamnă portalul european de căutare, astfel cum este menționat la articolul 6;

(34) „BMS comun” înseamnă serviciul comun de comparare a datelor biometrice, astfel cum este menționat la articolul 15;

(35) „CIR” înseamnă registrul comun de date de identitate, astfel cum este menționat la articolul 17;

(36) „MID” înseamnă detectorul de identități multiple, astfel cum este menționat la articolul 25;

(37) „CRRS” înseamnă registrul central de raportare și statistici, astfel cum este menționat la articolul 39.

Articolul 5
Nediscriminarea

Prelucrarea datelor cu caracter personal în sensul prezentului regulament nu conduce la discriminarea persoanelor pe motive de sex, rasă sau origine etnică, religie sau convingeri, handicap, vârstă sau orientare sexuală. Pe parcursul prelucrării datelor cu caracter personal se respectă pe deplin demnitatea și integritatea umană. Se acordă o atenție specială copiilor, persoanelor în vârstă și persoanelor cu handicap.

CAPITOLUL II
Portalul european de căutare

Articolul 6
Portalul european de căutare

1. Se instituie un portal european de căutare (ESP) cu scopul (i) de a asigura accesul rapid, neîntrerupt, eficient, sistematic și controlat al autorităților statelor membre și al organismelor UE la sistemele de informații ale UE, la datele Europol și la bazele de date ale Interpol de care au nevoie pentru a-și îndeplini sarcinile în conformitate cu drepturile de acces de care beneficiază și (ii) de a sprijini realizarea obiectivelor EES, VIS, [ETIAS], Eurodac, SIS, [ECRIS-TCN] și ale datelor Europol.

2. ESP este alcătuit din următoarele componente:

   (a) o infrastructură centrală, care include un portal de căutare ce permite lansarea de interogări simultane în EES, VIS, [ETIAS], Eurodac, SIS, [ECRIS-TCN], precum și în datele Europol și în bazele de date ale Interpol;

   (b) un canal securizat de comunicații între ESP, statele membre și organismele UE care au dreptul să utilizeze ESP în conformitate cu dreptul Uniunii;

   (c) o infrastructură de comunicații securizată între ESP și EES, VIS, [ETIAS], Eurodac, SIS central, [ECRIS-TCN], datele Europol și bazele de date ale Interpol, precum și între ESP și infrastructurile centrale ale registrului comun de date de identitate (CIR) și ale detectorului de identități multiple.

3. Agenția eu-LISA dezvoltă ESP și asigură gestionarea tehnică a acestuia.

Articolul 7
Utilizarea portalului european de căutare

1. Utilizarea ESP este rezervată autorităților statelor membre și organismelor UE care au acces la EES, [ETIAS], VIS, SIS, Eurodac și [ECRIS-TCN], la CIR și la detectorul de identități multiple, precum și la datele Europol și la bazele de date ale Interpol, în conformitate cu dreptul Uniunii sau cu dreptul național care reglementează un astfel de acces.

2. Autoritățile menționate la alineatul (1) utilizează ESP pentru a căuta date referitoare la persoane sau la documentele de călătorie ale acestora în sistemele centrale ale EES, VIS și [ETIAS], în conformitate cu drepturile de acces de care beneficiază în temeiul dreptului național și al Uniunii. De asemenea, acestea utilizează ESP pentru a lansa interogări în CIR în conformitate cu drepturile de acces de care beneficiază în temeiul prezentului regulament, în scopurile menționate la articolele 20, 21 și 22.

3. Autoritățile statelor membre menționate la alineatul (1) pot utiliza ESP pentru a căuta date referitoare la persoane sau la documentele de călătorie ale acestora în SIS central menționat în [Regulamentul privind SIS în domeniul verificărilor la frontiere și în Regulamentul privind SIS în domeniul asigurării respectării legii]. Accesul la SIS central prin intermediul ESP se face prin sistemele naționale (N.SIS) din fiecare stat membru, în conformitate cu [articolul 4 alineatul (2) din Regulamentul privind SIS în domeniul verificărilor la frontiere și din Regulamentul privind SIS în domeniul asigurării respectării legii].

4. Organismele UE utilizează ESP pentru a căuta date referitoare la persoane sau la documentele de călătorie ale acestora în SIS central.

5. Autoritățile menționate la alineatul (1) pot utiliza ESP pentru a căuta date referitoare la persoane sau la documentele de călătorie ale acestora în bazele de date ale Interpol, în conformitate cu drepturile de acces de care beneficiază în temeiul dreptului național și al Uniunii.

Articolul 8
Profiluri pentru utilizatorii portalului european de căutare

1. Pentru a facilita utilizarea ESP, eu-LISA creează un profil pentru fiecare categorie de utilizator al ESP, în conformitate cu detaliile tehnice și cu drepturile de acces menționate la alineatul (2), precum și cu dreptul Uniunii și cel național:

   (a) câmpurile de date care se utilizează pentru lansarea interogărilor;

   (b) sistemele de informații ale UE, datele Europol și bazele de date ale Interpol care sunt sau pot fi consultate și care oferă un răspuns utilizatorului și

   (c) datele furnizate în fiecare răspuns.

2. Comisia adoptă acte delegate în conformitate cu articolul 63 pentru a specifica detaliile tehnice ale profilurilor menționate la alineatul (1) pentru utilizatorii ESP menționați la articolul 7 alineatul (1), în conformitate cu drepturile lor de acces.

Articolul 9
Interogări

1. Utilizatorii ESP lansează o interogare prin introducerea de date în ESP în conformitate cu profilurile de utilizator ale acestora și cu drepturile de acces de care beneficiază. În cazul în care a fost lansată o interogare, ESP va interoga simultan, folosind datele introduse de utilizatorul ESP, următoarele sisteme: EES, [ETIAS], VIS, SIS, Eurodac, [ECRIS-TCN] și CIR, precum și datele Europol și bazele de date ale Interpol.

2. Câmpurile de date folosite pentru a lansa o interogare prin intermediul ESP corespund câmpurilor de date referitoare la persoane sau documente de călătorie care pot fi utilizate pentru a interoga diferitele sisteme de informații ale UE, datele Europol și bazele de date ale Interpol în conformitate cu instrumentele juridice care le reglementează.

3. Agenția eu-LISA întocmește pentru ESP un document de control al interfeței (ICD) pe baza formatului universal pentru mesaje (UMF) menționat la articolul 38.

4. EES, [ETIAS], VIS, SIS, Eurodac, [ECRIS-TCN], CIR și detectorul de identități multiple, precum și datele Europol și bazele de date ale Interpol furnizează datele pe care le conțin și care rezultă din interogarea ESP.

5. ESP trebuie conceput astfel încât, atunci când se lansează interogări în bazele de date ale Interpol, să se asigure faptul că datele utilizate de către utilizatorul ESP pentru a lansa o interogare nu sunt partajate cu proprietarii datelor Interpol.

6. Răspunsul furnizat utilizatorului ESP este unic și conține toate informațiile la care acesta are acces în temeiul dreptului Uniunii. Dacă este cazul, răspunsul furnizat de ESP indică sistemul de informații sau baza de date de unde provin datele.

7. Comisia adoptă un act delegat în conformitate cu articolul 63 pentru a preciza conținutul și formatul răspunsurilor ESP.

Articolul 10
Păstrarea înregistrărilor

1. Fără a aduce atingere [articolului 46 din Regulamentul privind EES], articolului 34 din Regulamentul (CE) nr. 767/2008, [articolului 59 din Propunerea privind ETIAS] și articolelor 12 și 18 din Regulamentul privind SIS în domeniul verificărilor la frontiere, eu-LISA păstrează înregistrări ale tuturor operațiunilor de prelucrare a datelor din cadrul ESP. În aceste înregistrări sunt incluse, în special, următoarele informații:

   (a) autoritatea statului membru și utilizatorul individual al ESP, inclusiv profilul ESP utilizat, astfel cum se menționează la articolul 8;

   (b) data și ora efectuării interogării;

   (c) sistemele de informații ale UE și datele de baze ale Interpol care au fost interogate;

   (d) în conformitate cu normele naționale sau, după caz, în conformitate cu Regulamentul (CE) nr. 45/2001, datele de identificare ale agentului care a efectuat interogarea.

2. Înregistrările 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 datelor în temeiul articolului 42. Aceste înregistrări sunt protejate prin măsuri corespunzătoare împotriva accesului neautorizat și sunt șterse după o perioadă de un an de la data la care au fost create, cu excepția cazului în care sunt necesare pentru desfășurarea unor proceduri de control aflate în curs.

Articolul 11
Proceduri alternative în cazul imposibilității tehnice de a utiliza portalul european de căutare

1. În cazul în care, din cauza unei disfuncționalități a ESP, este imposibil din punct de vedere tehnic să se utilizeze ESP pentru a lansa o interogare într-unul sau mai multe dintre sistemele de informații ale UE menționate la articolul 9 alineatul (1) sau în CIR, utilizatorii ESP primesc o notificare în acest sens din partea eu-LISA.

2. În cazul în care, din cauza unei disfuncționalități a infrastructurii naționale dintr-un stat membru, este imposibil din punct de vedere tehnic să se utilizeze ESP pentru a lansa o interogare într-unul sau mai multe dintre sistemele de informații ale UE menționate la articolul 9 alineatul (1) sau în CIR, autoritatea competentă a respectivului stat membru notifică eu-LISA și Comisia.

3. În ambele scenarii, și până la remedierea problemei tehnice, obligația menționată la articolul 7 alineatele (2) și (4) nu se aplică, iar statele membre pot avea acces la sistemele de informații menționate la articolul 9 alineatul (1) sau la CIR în mod direct, utilizând propriile interfețe naționale uniforme sau infrastructurile de comunicații naționale.

CAPITOLUL III
Serviciul comun de comparare a datelor biometrice

Articolul 12
Serviciul comun de comparare a datelor biometrice

1. Pentru a sprijini CIR și detectorul de identități multiple și obiectivele EES, VIS, Eurodac, SIS și [ECRIS-TCN], se instituie un serviciu comun de comparare a datelor biometrice (BMS comun), care stochează modele biometrice și permite efectuarea de interogări folosind date biometrice în mai multe sisteme de informații ale UE.

2. BMS comun este alcătuit din următoarele componente:

   (a) o infrastructură centrală, care include un motor de căutare și spațiul de stocare a datelor menționate la articolul 13;

   (b) o infrastructură de comunicații securizată între BMS comun, SIS central și CIR.

3. Agenția eu-LISA dezvoltă BMS comun și asigură gestionarea tehnică a acestuia.

Articolul 13
Datele stocate în serviciul comun de comparare a datelor biometrice

1. În BMS comun se stochează modele biometrice pe care acesta le generează din următoarele date biometrice:

   (a) datele menționate la articolul 16 alineatul (1) litera (d) și la articolul 17 alineatul (1) literele (b) și (c) din Regulamentul (UE) 2017/2226;

   (b) datele menționate la articolul 9 alineatul (6) din Regulamentul (CE) nr. 767/2008;

   (c) [datele menționate la articolul 20 alineatul (2) literele (w) și (x) din Regulamentul privind SIS în domeniul verificărilor la frontiere;

   (d) datele menționate la articolul 20 alineatul (3) literele (w) și (x) din Regulamentul privind SIS în domeniul asigurării respectării legii;

   (e) datele menționate la articolul 4 alineatul (3) literele (t) și (u) din Regulamentul privind SIS în domeniul returnării ilegale];

   (f) [datele menționate la articolul 13 litera (a) din Regulamentul privind Eurodac;]

   (g) [datele menționate la articolul 5 alineatul (1) litera (b) și la articolul 5 alineatul (2) din Regulamentul privind ECRIS-TCN.]

2. BMS comun include în fiecare model biometric o trimitere la sistemele de informații în care sunt stocate datele biometrice corespondente.

3. Modelele biometrice se introduc în BMS comun numai în urma unei verificări automatizate a calității datelor biometrice adăugate într-unul din sistemele de informații, efectuate de BMS comun pentru a se asigura îndeplinirea unui standard minim de calitate a datelor.

4. Stocarea datelor menționate la alineatul (1) respectă standardele de calitate prevăzute la articolul 37 alineatul (2).

Articolul 14

Căutarea de date biometrice prin intermediul serviciului comun de comparare a datelor biometrice

Pentru a căuta date biometrice stocate în CIR și SIS, CIR și SIS utilizează modelele biometrice stocate în BMS comun. Interogările efectuate folosind date biometrice se lansează în conformitate cu scopurile prevăzute în prezentul regulament și în Regulamentul privind EES, Regulamentul privind VIS, Regulamentul privind Eurodac, [Regulamentele privind SIS] și [Regulamentul privind ECRIS-TCN].

Articolul 15

Păstrarea datelor în serviciul comun de comparare a datelor biometrice

Datele menționate la articolul 13 sunt stocate în BMS comun atât timp cât sunt stocate în CIR sau SIS datele biometrice corespondente.

Articolul 16

Păstrarea înregistrărilor

1. Fără a aduce atingere [articolului 46 din Regulamentul privind EES], articolului 34 din Regulamentul (CE) nr. 767/2008 și [articolelor 12 și 18 din Regulamentul privind SIS în domeniul asigurării respectării legii], eu-LISA păstrează înregistrările tuturor operațiunilor de prelucrare a datelor efectuate în BMS comun. În aceste înregistrări sunt incluse, în special, următoarele informații:

   (a) istoricul referitor la crearea și stocarea modelelor biometrice;

   (b) o trimitere la sistemele de informații ale UE în care s-au efectuat interogările folosind modelele biometrice stocate în BMS comun;

   (c) data și ora efectuării interogării;

   (d) tipul de date biometrice utilizate pentru lansarea interogării;

   (e) durata interogării;

   (f) rezultatele interogării și data și ora obținerii rezultatului;

   (g) în conformitate cu normele naționale sau, după caz, în conformitate cu Regulamentul (CE) nr. 45/2001, datele de identificare ale agentului care a efectuat interogarea.

2. Înregistrările 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 datelor în temeiul articolului 42. Aceste înregistrări sunt protejate prin măsuri corespunzătoare împotriva accesului neautorizat și sunt șterse după o perioadă de un an de la data la care au fost create, cu excepția cazului în care sunt necesare pentru desfășurarea unor proceduri de control aflate în curs. Înregistrările menționate la alineatul 1 litera (a) sunt șterse de îndată ce sunt șterse datele.

CAPITOLUL IV
Registrul comun de date de identitate

Articolul 17

Registrul comun de date de identitate

1. Se instituie un registru comun de date de identitate (CIR), în care se creează un dosar individual pentru fiecare persoană care este înregistrată în EES, VIS, [ETIAS], Eurodac

sau [ECRIS-TCN], ce conține datele menționate la articolul 18, în scopul de a facilita și a asista procesul de identificare corectă a persoanelor înregistrate în EES, VIS, [ETIAS], Eurodac și [ECRIS-TCN], de a sprijini funcționarea detectorului de identități multiple și de a facilita și simplifica accesul autorităților de aplicare a legii la sistemele de informații care nu intră în sfera asigurării respectării legii la nivelul UE, atunci când acest lucru este necesar pentru prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor grave.

2. CIR este alcătuit din următoarele componente:

(a) o infrastructură centrală care va înlocui sistemele centrale ale EES, VIS, [ETIAS], Eurodac și, respectiv, [ECRIS-TCN], în măsura în care aceasta va stoca datele menționate la articolul 18;

(b) un canal securizat de comunicații între CIR, statele membre și organismele UE care au dreptul să utilizeze portalul european de căutare (ESP) în conformitate cu dreptul Uniunii;

(c) o infrastructură de comunicații securizată între CIR și EES, [ETIAS], VIS, Eurodac și [ECRIS-TCN], precum și cu infrastructurile centrale ale ESP, BMS comun și detectorul de identități multiple.

3. Agenția eu-LISA dezvoltă CIR și asigură gestionarea tehnică a acestuia.

Articolul 18
Datele din registrul comun de date de identitate

1. CIR stochează următoarele date, separate în mod logic, în funcție de sistemul de informații din care provin datele:

(a) datele menționate la [articolul 16 alineatul (1) literele (a)-(d) și la articolul 17 alineatul (1) literele (a)-(c) din Regulamentul privind EES];

(b) datele menționate la articolul 9 alineatul (4) literele (a)-(c) și alineatele (5) și (6) din Regulamentul (CE) nr. 767/2008;

(c) [datele menționate la articolul 15 alineatul (2) literele (a)-(e) din Regulamentul privind ETIAS;]

(d) – (nu se aplică)

(e) – (nu se aplică)

2. Pentru fiecare set de date menționate la alineatul (1), CIR include o trimitere la sistemele de informații din care provin datele.

3. Stocarea datelor menționate la alineatul (1) respectă standardele de calitate prevăzute la articolul 37 alineatul (2).

Articolul 19
Adăugarea, modificarea și ștergerea datelor din registrul comun de date de identitate

1. În cazul în care se adaugă, se modifică sau se elimină date din EES, VIS și [ETIAS], datele menționate la articolul 18 stocate în dosarul individual din CIR se adăugă, se modifică sau se elimină în mod automat.

2. În cazul în care detectorul de identități multiple creează o conexiune albă sau roșie, în conformitate cu articolele 32 și 33, între datele provenite din două sau mai multe dintre

sistemele de informații ale UE care alcătuiesc CIR, în loc să se creeze un nou dosar individual, CIR adaugă datele noi în dosarul individual al datelor conexate.

Articolul 20
Accesul la registrul comun de date de identitate în scopul identificării

1. În cazul în care o autoritate de poliție a unui stat membru are competențe în acest sens în temeiul unor măsuri legislative naționale, astfel cum se menționează la alineatul (2), aceasta poate, exclusiv în scopul identificării unei persoane, să lanseze o interogare în CIR folosind datele biometrice ale persoanei respective, preluate în cursul unui control de identitate.

   În cazul în care, în urma interogării, reiese că în CIR sunt stocate date referitoare la persoana respectivă, autoritatea statului membru are acces să consulte datele menționate la articolul 18 alineatul (1).

   În cazul în care datele biometrice ale persoanei respective nu pot fi utilizate sau interogarea lansată folosind acele date nu a dat rezultate, se lansează o interogare cu datele de identitate ale persoanei, în combinație cu datele din documentul de călătorie sau cu datele de identitate pe care le furnizează persoana respectivă.

2. Statele membre care doresc să facă uz de posibilitatea prevăzută la prezentul articol adoptă în acest sens măsuri legislative naționale. Aceste măsuri legislative precizează scopurile precise ale controalelor de identitate din cele menționate la articolul 2 alineatul (1) literele (b) și (c). Statele membre desemnează autoritățile de poliție competente și stabilesc procedurile, condițiile și criteriile aferente acestor controale.

Articolul 21
Accesul la registrul comun de date de identitate în scopul detectării de identități multiple

1. În cazul în care o interogare în CIR are ca rezultat o conexiune galbenă, în conformitate cu articolul 28 alineatul (4), autoritatea responsabilă de verificarea identităților diferite, stabilită în conformitate cu articolul 29, are acces, exclusiv în scopul verificării respective, la datele stocate în CIR aparținând diferitelor sisteme de informații conexate printr-o conexiune galbenă.

2. În cazul în care o interogare în CIR are ca rezultat o conexiune roșie, în conformitate cu articolul 32, autoritățile menționate la articolul 26 alineatul (2) au acces, exclusiv în scopul combaterii fraudei de identitate, la datele stocate în CIR aparținând diferitelor sisteme de informații conexate printr-o conexiune roșie.

Articolul 22
Efectuarea de interogări în registrul comun de date de identitate în scopul asigurării respectării legii

1. În scopul prevenirii, depistării și investigării infracțiunilor de terorism sau a altor infracțiuni grave într-un anumit caz și pentru a obține informații cu privire la existența sau nu a unor date referitoare la o anumită persoană în EES, VIS și [ETIAS], autoritățile desemnate ale statelor membre și Europol pot consulta CIR.

2. Autoritățile desemnate ale statelor membre și Europol nu au dreptul să consulte datele din [ECRIS-TCN] atunci când consultă CIR în scopurile menționate la alineatul (1).

3. În cazul în care rezultatul unei interogări în CIR indică faptul că există date privind persoana respectivă în EES, VIS și [ETIAS], CIR pune la dispoziția autorităților desemnate ale statelor membre și a Europol un răspuns sub forma unei trimiteri, indicând în care dintre sistemele de informații există datele între care s-a stabilit o concordanță menționate la articolul 18 alineatul (2). Răspunsul CIR este formulat astfel încât securitatea datelor să nu fie compromisă.

4. Accesul deplin la datele conținute în sistemele de informații ale UE în scopul prevenirii, depistării și investigării infracțiunilor cu caracter terorist sau a altor infracțiuni grave rămâne supus condițiilor și procedurilor prevăzute în instrumentele legislative respective care reglementează acest acces.

Articolul 23
Păstrarea datelor în registrul comun de date de identitate

1. Datele menționate la articolul 18 alineatele (1) și (2) se elimină din CIR în conformitate cu dispozițiile privind păstrarea datelor din [Regulamentul privind EES], Regulamentul privind VIS și, respectiv, [Regulamentul privind ETIAS].

2. Dosarul individual este stocat în CIR atât timp cât datele corespondente sunt stocate cel puțin într-unul din sistemele de informații ale căror date sunt incluse în CIR. Crearea unei conexiuni nu afectează durata de păstrare a fiecărui element al datelor conexate.

Articolul 24
Păstrarea înregistrărilor

1. Fără a aduce atingere [articolului 46 din Regulamentul privind EES,] articolului 34 din Regulamentul (CE) nr. 767/2008 [și articolului 59 din propunerea privind ETIAS], eu-LISA păstrează înregistrări ale tuturor operațiunilor de prelucrare a datelor efectuate în CIR, în conformitate cu alineatele (2), (3) și (4).

2. În ceea ce privește accesul la CIR în temeiul articolului 20, eu-LISA păstrează înregistrările tuturor operațiunilor de prelucrare a datelor efectuate în CIR. În aceste înregistrări sunt incluse, în special, următoarele informații:

   (a) scopul accesului utilizatorului care a lansat interogarea în CIR;

   (b) data și ora efectuării interogării;

   (c) tipul de date utilizate pentru lansarea interogării;

   (d) rezultatele interogării;

   (e) în conformitate cu normele naționale sau cu Regulamentul (UE) 2016/794 ori, după caz, cu Regulamentul (CE) nr. 45/2001, datele de identificare ale agentului care a efectuat interogarea.

3. În ceea ce privește accesul la CIR în temeiul articolului 21, eu-LISA păstrează înregistrările tuturor operațiunilor de prelucrare a datelor efectuate în CIR. În aceste înregistrări sunt incluse, în special, următoarele informații:

   (a) scopul accesului utilizatorului care a lansat interogarea în CIR;

   (b) data și ora efectuării interogării;

   (c) atunci când este relevant, datele utilizate pentru lansarea interogării;

   (d) atunci când este relevant, rezultatele interogării;

   (e) în conformitate cu normele naționale sau cu Regulamentul (UE) 2016/794 ori, după caz, cu Regulamentul (CE) nr. 45/2001, datele de identificare ale agentului care a

efectuat interogarea.

4. În ceea ce privește accesul la CIR în temeiul articolului 22, eu-LISA păstrează înregistrările tuturor operațiunilor de prelucrare a datelor efectuate în CIR. În aceste înregistrări sunt incluse, în special, următoarele informații:

   (a) referința dosarului național;

   (b) data și ora efectuării interogării;

   (c) tipul de date utilizate pentru lansarea interogării;

   (d) rezultatele interogării;

   (e) numele autorității care a consultat CIR;

   (f) în conformitate cu normele naționale sau cu Regulamentul (UE) 2016/794 sau, după caz, cu Regulamentul (CE) nr. 45/2001, datele de identificare ale agentului care a efectuat interogarea și ale agentului care a dispus interogarea.

   Înregistrările acestor accesări sunt verificate periodic de autoritatea de supraveghere competentă stabilită în conformitate cu articolul 51 din Regulamentul (UE) 2016/679 sau în conformitate cu articolul 41 din Directiva 2016/680, la intervale de cel mult șase luni, pentru a verifica dacă sunt îndeplinite procedurile și condițiile prevăzute la articolul 22 alineatele (1)-(3).

5. Fiecare stat membru păstrează înregistrările interogărilor efectuate de personalul autorizat în mod corespunzător să utilizeze CIR în temeiul articolelor 20, 21 și 22.

6. Înregistrările menționate la alineatele (1) și (5) 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 datelor în conformitate cu articolul 42. Înregistrările sunt protejate prin măsuri corespunzătoare împotriva accesului neautorizat și sunt șterse după o perioadă de un an, cu excepția cazului în care sunt necesare pentru desfășurarea unor proceduri de control aflate în curs.

7. Agenția eu-LISA păstrează înregistrările referitoare la istoricul datelor stocate în dosarul individual, în scopul definit la alineatul (6). Înregistrările legate de istoricul datelor stocate se șterg de îndată ce sunt șterse datele.

CAPITOLUL V
Detectorul de identități multiple

Articolul 25
Detectorul de identități multiple

1. Pentru a susține funcționarea CIR și a sprijini realizarea obiectivelor EES, VIS, [ETIAS], Eurodac, SIS și [ECRIS-TCN], se instituie un detector de identități multiple (MID), care creează și stochează conexiuni între datele din sistemele de informații ale UE incluse în registrul comun de date de identitate (CIR) și SIS, detectând astfel identitățile multiple, cu scopul dublu de a facilita controalele de identitate și de a combate frauda de identitate.

2. MID este alcătuit din următoarele componente:

   (a) o infrastructură centrală, care stochează conexiuni și trimiteri la sistemele de informații;

(b) o infrastructură de comunicații securizată, care conectează MID cu SIS, cu infrastructurile centrale ale portalului european de căutare și cu CIR.

3. Agenția eu-LISA dezvoltă MID și asigură gestionarea tehnică a acestuia.

Articolul 26
Accesul la detectorul de identități multiple

1. În scopul verificării manuale a identității, menționate la articolul 29, se acordă acces la datele menționate la articolul 34 stocate în MID:

(a) autorităților de frontieră atunci când creează sau actualizează un dosar individual, astfel cum se prevede la articolul 14 din [Regulamentul privind EES];

(b) autorităților competente menționate la articolul 6 alineatele (1) și (2) din Regulamentul 767/2008 atunci când creează sau actualizează un dosar de cerere în VIS în conformitate cu articolul 8 din Regulamentul (CE) nr. 767/2008;

(c) [unității centrale a ETIAS și unităților naționale ale ETIAS atunci când efectuează evaluarea menționată la articolele 20 și 22 din Regulamentul privind ETIAS;]

(d) – (nu se aplică);

(e) birourilor SIRENE din statul membru atunci când creează [o semnalare SIS în conformitate cu Regulamentul privind SIS în domeniul verificărilor la frontiere];

(f) – (nu se aplică).

2. Autoritățile statelor membre și organismele UE care au acces la cel puțin un sistem de informații al UE inclus în *registrul comun de date de identitate sau la SIS* au acces la datele menționate la articolul 34 literele (a) și (b) cu privire la orice conexiune roșie, astfel cum se menționează la articolul 32.

Articolul 27
Detectarea de identități multiple

1. Se lansează o detectare de identități multiple în registrul comun de date de identitate și în SIS atunci când:

(a) se creează sau se actualizează un dosar individual în [EES, în conformitate cu articolul 14 din Regulamentul privind EES];

(b) se creează sau se actualizează un dosar de cerere în VIS în conformitate cu articolul 8 din Regulamentul (CE) nr. 767/2008;

(c) [se creează sau se actualizează un dosar de cerere în ETIAS în conformitate cu articolul 17 din Regulamentul privind ETIAS;]

(d) – (nu se aplică);

(e) [se creează sau se actualizează o semnalare în SIS privind o persoană, în conformitate cu dispozițiile capitolului V din Regulamentul privind SIS în domeniul verificărilor la frontiere];

(f) – (nu se aplică).

2. În cazul în care datele conținute într-unul dintre sistemele de informații menționate la alineatul (1) includ date biometrice, registrul comun de date de identitate (CIR) și SIS central utilizează serviciul comun de comparare a datelor biometrice (BMS comun) pentru a detecta identitățile multiple. BMS comun compară modelele biometrice obținute din

eventualele date biometrice noi cu modelele biometrice existente în BMS comun pentru a verifica dacă sunt deja stocate în CIR sau în SIS central date care aparțin aceluiași resortisant al unei țări terțe.

3. În plus față de procesul menționat la alineatul (2), CIR și SIS central utilizează portalul european de căutare pentru a căuta datele stocate în CIR și în SIS central utilizând următoarele date:

(a) numele de familie; prenumele; data nașterii, sexul și cetățenia (cetățeniile), astfel cum se menționează la articolul 16 alineatul (1) litera (a) din [Regulamentul privind EES];

(b) numele de familie; prenumele; data nașterii, sexul și cetățenia (cetățeniile), astfel cum se menționează la articolul 9 alineatul (4) litera (a) din Regulamentul (CE) nr. 767/2008;

(c) [numele de familie; prenumele; numele de familie la naștere; data nașterii, locul nașterii, sexul și cetățenia (cetățeniile), astfel cum se menționează la articolul 15 alineatul (2) din Regulamentul privind ETIAS;]

(d) – (nu se aplică);

(e) [numele de familie; prenumele; numele la naștere, numele folosite anterior și numele de împrumut; data nașterii, locul nașterii, cetățenia (cetățeniile) și sexul, astfel cum se prevede la articolul 20 alineatul (2) din Regulamentul privind SIS în domeniul verificărilor la frontiere;]

(f) – (nu se aplică);

(g) – (nu se aplică);

(h) – (nu se aplică).

4. Detectarea de identități multiple este lansată doar pentru a compara datele disponibile într-un sistem de informații cu datele disponibile în alte sisteme de informații.

Articolul 28
Rezultatele detectării de identități multiple

1. În cazul în care, în urma interogărilor menționate la articolul 27 alineatele (2) și (3), nu se obține un rezultat pozitiv, procedurile menționate la articolul 27 alineatul (1) continuă în conformitate cu regulamentele corespunzătoare care le reglementează.

2. În cazul în care, în urma interogărilor menționate la articolul 27 alineatele (2) și (3), se obține(e) unul sau mai multe rezultate pozitive, registrul comun de date de identitate și, dacă este relevant, SIS creează o conexiune între datele utilizate pentru lansarea interogării și datele care au generat rezultatul pozitiv.

În cazul în care se obțin mai multe rezultate pozitive, se creează o conexiune între toate datele care au generat rezultatul pozitiv. În cazul în care datele erau deja conexate, conexiunea existentă se extinde la datele utilizate pentru lansarea interogării.

3. În cazul în care, în urma interogării menționate la articolul 27 alineatul (2) sau (3), se obține(e) unul sau mai multe rezultate pozitive și datele de identitate din dosarele conexate sunt identice sau similare, se creează o conexiune albă în conformitate cu articolul 33.

4. În cazul în care, în urma interogării menționate la articolul 27 alineatul (2) sau (3), se obține(e) unul sau mai multe rezultate pozitive și datele de identitate din dosarele legate nu pot fi considerate ca fiind similare, se creează o conexiune galbenă în conformitate cu articolul 30 și se aplică procedura prevăzută la articolul 29.

5. Comisia stabilește, prin acte de punere în aplicare, proceduri pentru a stabili cazurile în care datele de identitate pot fi considerate identice sau similare. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 64 alineatul (2).

6. Conexiunile sunt stocate în dosarul de confirmare a identității menționat la articolul 34.

Comisia stabilește, prin acte de punere în aplicare, normele tehnice de conexare a datelor provenite de la diferitele sisteme de informații. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 64 alineatul (2).

Articolul 29
Verificarea manuală a identităților diferite

1. Fără a aduce atingere alineatului (2), autoritatea responsabilă de verificarea identităților diferite este:

   (a) autoritatea de frontieră în cazul rezultatelor pozitive obținute la crearea sau actualizarea unui dosar individual în [EES în conformitate cu articolul 14 din Regulamentul privind EES];

   (b) autoritățile competente menționate la articolul 6 alineatele (1) și (2) din Regulamentul 767/2008 în cazul rezultatelor pozitive obținute la crearea sau actualizarea unui dosar de cerere în VIS în conformitate cu articolul 8 din Regulamentul (CE) nr. 767/2008;

   (c) [unitatea centrală a ETIAS și unitățile naționale ale ETIAS în cazul rezultatelor pozitive obținute în conformitate cu articolele 18, 20 și 22 din Regulamentul privind ETIAS;]

   (d) – (nu se aplică);

   (e) birourile SIRENE din statul membru în cazul rezultatelor pozitive obținute la crearea unei semnalări în SIS în conformitate cu [Regulamentul privind SIS în domeniul verificărilor la frontiere];

   (f) – (nu se aplică).

   Detectorul de identități multiple indică autoritatea responsabilă de verificarea identităților diferite în dosarul de verificare a identității.

2. Autoritatea responsabilă de verificarea identităților diferite în dosarul de confirmare a identității este biroul SIRENE din statul membru care a creat semnalarea, în cazul în care se stabilește o conexiune între datele conținute:

   (a) într-o semnalare cu privire la persoanele căutate pentru a fi arestate în vederea predării sau a extrădării, astfel cum se prevede la articolul 26 din [Regulamentul privind SIS în domeniul asigurării respectării legii];

   (b) într-o semnalare cu privire la persoane dispărute sau vulnerabile, astfel cum se prevede la articolul 32 din [Regulamentul privind SIS în domeniul asigurării respectării legii];

   (c) într-o semnalare cu privire la persoane căutate în vederea participării la o procedură judiciară, astfel cum se prevede la articolul 34 din [Regulamentul privind SIS în domeniul asigurării respectării legii];

   (d) [într-o semnalare privind returnarea, în conformitate cu Regulamentul privind SIS în

domeniul returnării ilegale];

(e) într-o semnalare cu privire la persoane în scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice, astfel cum se prevede la articolul 36 din [Regulamentul privind SIS în domeniul asigurării respectării legii];

(f) într-o semnalare cu privire la persoane căutate necunoscute în scopul identificării în conformitate cu dreptul național și al căutării cu ajutorul datelor biometrice, astfel cum se prevede la articolul 40 din [Regulamentul privind SIS în domeniul asigurării respectării legii].

3. Fără a aduce atingere alineatului (4), autoritatea responsabilă de verificarea identităților diferite are acces la datele conținute în dosarul relevant de confirmare a identității și la datele de identitate conexate din registrul comun de date de identitate și, în cazul în care este relevant, din SIS, evaluează identitățile diferite și actualizează conexiunea în conformitate cu articolele 31, 32 și 33 și o adaugă fără întârziere la dosarul de confirmare a identității.

4. În cazul în care autoritatea responsabilă de verificarea identităților diferite în dosarul de confirmare a identității este autoritatea de frontieră care a creat sau a actualizat un dosar individual în EES în conformitate cu articolul 14 din Regulamentul privind EES și în cazul în care se obține o conexiune galbenă, autoritatea de frontieră efectuează verificări suplimentare în cadrul unei verificări în linia a doua. Pe parcursul acestei verificări în linia a doua, autoritățile de frontieră au acces la datele relevante conținute în dosarul de confirmare a identității relevant, evaluează identitățile diferite și actualizează conexiunea în conformitate cu articolele 31-33 și o adaugă fără întârziere la dosarul de confirmare a identității.

5. În cazul în care se obțin mai multe conexiuni, autoritatea responsabilă de verificarea identităților diferite evaluează fiecare conexiune separat.

6. În cazul în care datele care au generat răspunsul pozitiv erau deja conexate, autoritatea responsabilă de verificarea identităților diferite ține seama de conexiunile existente atunci când evaluează crearea de noi conexiuni.

Articolul 30
Conexiune galbenă

1. O conexiune între datele din două sau mai multe sisteme de informații este clasificată ca galbenă în oricare dintre următoarele cazuri:

(a) datele conexate au aceleași date biometrice, însă date de identitate diferite și nu s-a efectuat o verificare manuală a identităților diferite;

(b) datele conexate au date de identitate diferite și nu s-a efectuat o verificare manuală a identităților diferite.

2. În cazul în care o conexiune este clasificată ca galbenă în conformitate cu alineatul (1), se aplică procedura prevăzută la articolul 29.

Articolul 31
Conexiune verde

1. O conexiune între datele din două sau mai multe sisteme de informații este clasificată ca verde în cazul în care datele conexate nu au aceleași date biometrice, însă au date de

identitate similare, iar autoritatea responsabilă de verificarea identităților diferite a ajuns la concluzia că datele se referă la două persoane diferite.

2. În cazul în care se lansează o interogare în registrul comun de date de identitate (CIR) sau în SIS și există o conexiune verde între două sau mai multe dintre sistemele de informații care formează CIR sau între acestea și SIS, detectorul de identități multiple indică faptul că datele de identitate ale datelor conexate nu corespund aceleiași persoane. Sistemul de informații în care s-a lansat interogarea răspunde indicând doar datele persoanei ale cărei date au fost utilizate pentru interogare, fără a genera un rezultat pozitiv în raport cu datele care formează conexiunea verde.

Articolul 32
Conexiune roșie

1. O conexiune între datele din două sau mai multe sisteme de informații este clasificată ca roșie în oricare dintre următoarele cazuri:

   (a) datele conexate au aceleași date biometrice, însă date de identitate diferite, iar autoritatea responsabilă de verificarea identităților diferite a ajuns la concluzia că datele se referă în mod ilegal la aceeași persoană;

   (b) datele conexate au date de identitate similare și autoritatea responsabilă de verificarea identităților diferite a ajuns la concluzia că datele se referă în mod ilegal la aceeași persoană.

2. În cazul în care se lansează o interogare în CIR sau în SIS și există o conexiune roșie între două sau mai multe dintre sistemele de informații care formează CIR sau între acestea și SIS, detectorul de identități multiple răspunde indicând datele menționate la articolul 34. Măsurile subsecvente creării unei conexiuni roșii se iau în conformitate cu dreptul Uniunii și cu dreptul național.

3. În cazul în care este creată o conexiune roșie între datele din EES, VIS, [ETIAS], Eurodac sau [ECRIS-TCN], dosarul individual stocat în CIR se actualizează în conformitate cu articolul 19 alineatul (1).

4. Fără a aduce atingere dispozițiilor referitoare la gestionarea semnalărilor în SIS menționate în [Regulamentele privind SIS în domeniul verificărilor la frontiere, în domeniul asigurării respectării legii și în domeniul returnării ilegale] și fără a aduce atingere restricțiilor necesare pentru protejarea securității și a ordinii publice, pentru prevenirea infracțiunilor și pentru garantarea faptului că nicio anchetă națională nu va fi pusă în pericol, în cazul în care se creează o conexiune roșie, autoritatea responsabilă de verificarea identităților diferite informează persoana cu privire la prezența identităților multiple ilegale.

5. În cazul în care se creează o conexiune roșie, autoritatea responsabilă de verificarea identităților diferite furnizează o referință autorităților responsabile de datele conexate.

Articolul 33
Conexiune albă

1. O conexiune între datele din două sau mai multe sisteme de informații este clasificată ca albă în oricare dintre următoarele cazuri:

   (a) datele conexate au aceleași date biometrice și date de identitate identice sau similare;

   (b) datele conexate au date de identitate identice sau similare și cel puțin unul dintre sistemele de informații nu dispune de datele biometrice ale persoanei în cauză;

(c) datele conexate au aceleași date biometrice, însă date de identitate diferite, iar autoritatea responsabilă de verificarea identităților diferite a ajuns la concluzia că datele se referă la aceeași persoană care are în mod legal date de identitate diferite.

2. În cazul în care se lansează o interogare în CIR sau în SIS și există o conexiune albă între două sau mai multe dintre sistemele de informații care formează CIR sau între acestea și SIS, detectorul de identități multiple indică faptul că datele de identitate ale datelor conexe corespund aceleiași persoane. Sistemele de informații în care s-a lansat interogarea răspund indicând, după caz, toate datele conexate referitoare la persoana respectivă și generând, prin urmare, un rezultat pozitiv în raport cu datele care formează conexiunea albă, dacă autoritatea care a lansat interogarea are acces la datele conexate în temeiul dreptului Uniunii sau al dreptului național.

3. În cazul în care se creează o conexiune albă între datele din EES, VIS, [ETIAS], Eurodac sau [ECRIS-TCN], dosarul individual stocat în CIR se actualizează în conformitate cu articolul 19 alineatul (1).

4. Fără a aduce atingere dispozițiilor referitoare la gestionarea semnalărilor în SIS menționate în [Regulamentele privind SIS în domeniul verificărilor la frontiere, în domeniul asigurării respectării legii și în domeniul returnării ilegale], în cazul în care este creată o conexiune albă în urma unei verificări manuale a unor identități multiple, autoritatea responsabilă de verificarea identităților diferite informează persoana cu privire la prezența unor discrepanțe între datele sale cu caracter personal stocate în sistemele respective și furnizează o referință autorităților responsabile de datele conexate.

Articolul 34
Dosarul de confirmare a identității

Dosarul de confirmare a identității conține următoarele date:

(a) conexiunile, inclusiv menționarea culorii, astfel cum se menționează la articolele 30-33;

(b) o trimitere la sistemele de informații ale căror date sunt conexate;

(c) un număr de identificare unic care permite extragerea datelor din sistemele de informații în care se află dosarele conexate corespondente;

(d) dacă este cazul, autoritatea responsabilă de verificarea identităților diferite.

Articolul 35
Păstrarea datelor în detectorul de identități multiple

Dosarul de confirmare a identității și datele din acest dosar, inclusiv conexiunile, se stochează în detectorul de identități multiple (MID) numai atât timp cât datele conexate sunt stocate în două sau mai multe dintre sistemele de informații ale UE.

Articolul 36
Păstrarea înregistrărilor

1. Agenția eu-LISA păstrează înregistrări ale tuturor operațiunilor de prelucrare a datelor efectuate în MID. În aceste înregistrări sunt incluse, în special, următoarele informații:

(a) scopul în care utilizatorul a avut acces și drepturile de acces ale acestuia;

(b) data și ora efectuării interogării;

(c) tipul de date utilizate pentru lansarea interogării (interogărilor);

(d) trimiterea la datele conexate;

(e) istoricul dosarului de confirmare a identității;

(f) datele de identificare ale agentului care a efectuat interogarea.

2. Fiecare stat membru păstrează înregistrări ale personalului autorizat în mod corespunzător să utilizeze MID.

3. Înregistrările 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 datelor în temeiul articolului 42. Înregistrările sunt protejate prin măsuri corespunzătoare împotriva accesului neautorizat și sunt șterse după o perioadă de un an de la data la care au fost create, cu excepția cazului în care sunt necesare pentru desfășurarea unor proceduri de control aflate în curs. Înregistrările legate de istoricul dosarului de confirmare a identității se șterg de îndată ce sunt șterse datele din dosarul de confirmare a identității.

CAPITOLUL VI
Măsuri de asistare a interoperabilității

Articolul 37
Calitatea datelor

1. Agenția eu-LISA instituie mecanisme și proceduri automate de control al calității datelor în ceea ce privește datele stocate în EES, [ETIAS], VIS, SIS, serviciul comun de comparare a datelor biometrice (BMS comun), registrul comun de date de identitate (CIR) și detectorul de identități multiple (MID).

2. Agenția eu-LISA instituie indicatori comuni de calitate a datelor și standarde minime de calitate pentru stocarea datelor în EES, [ETIAS], VIS, SIS, BMS comun, CIR și MID.

3. Agenția eu-LISA furnizează statelor membre rapoarte periodice privind mecanismele și procedurile automate de control al calității datelor și privind indicatorii comuni de calitate a datelor. De asemenea, agenția furnizează Comisiei rapoarte periodice privind problemele întâmpinate și statele membre vizate.

4. Detaliile privind mecanismele și procedurile automate de control al calității datelor și privind indicatorii comuni de calitate a datelor și standardele minime de calitate pentru stocarea datelor în EES, [ETIAS], VIS, SIS, BMS comun, CIR și MID, în special în ceea ce privește datele biometrice, sunt stabilite prin acte de punere în aplicare. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 64 alineatul (2).

5. La un an de la instituirea mecanismelor și procedurilor automate de control al calității datelor și a indicatorilor comuni de calitate a datelor și, ulterior, în fiecare an, Comisia evaluează modul în care statele membre asigură calitatea datelor și formulează eventuale recomandări. Statele membre pun la dispoziția Comisiei un plan de acțiune pentru remedierea deficiențelor identificate în raportul de evaluare și prezintă un raport cu privire la progresele înregistrate în funcție de acest plan de acțiune până în momentul în care acesta este pus în aplicare pe deplin. Comisia transmite raportul de evaluare Parlamentului

European, Consiliului, Autorității Europene pentru Protecția Datelor și Agenției pentru Drepturi Fundamentale a Uniunii Europene instituită prin Regulamentul (CE) nr. 168/2007 al Consiliului[75].

Articolul 38
Formatul universal pentru mesaje

1. Se instituie un format universal pentru mesaje (UMF). UMF definește standardele pentru anumite elemente de conținut ale schimbului transfrontalier de informații între sistemele de informații, autoritățile și/sau organizațiile participante din domeniul justiției și afacerilor interne.

2. Standardul UMF se utilizează în dezvoltarea EES, a [ETIAS], a portalului european de căutare, a CIR, a MID și, dacă este necesar, în dezvoltarea de către eu-LISA sau de către orice alt organism al UE a unor noi modele de schimb de informații și sisteme de informații în domeniul justiției și afacerilor interne.

3. Aplicarea standardului UMF poate fi avută în vedere în VIS, SIS și în orice model de schimb transfrontalier de informații și sistem de informații în domeniul justiției și afacerilor interne, nou sau existent, elaborat de statele membre sau de țările asociate.

4. Comisia adoptă un act de punere în aplicare pentru a stabili și dezvolta standardul UMF menționat la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 64 alineatul (2).

Articolul 39
Registrul central de raportare și statistici

1. Se instituie un registru central de raportare și statistici (CRRS) în scopul de a susține obiectivele EES, VIS, [ETIAS] și SIS și de a genera date statistice transsistemice și rapoarte analitice în scop operațional, de elaborare a politicilor și de asigurare a calității datelor.

2. Agenția eu-LISA creează, implementează și găzduiește CRRS în siturile sale tehnice care conțin datele menționate la [articolul 63 din Regulamentul privind EES], articolul 17 din Regulamentul (CE) nr. 767/2008, [articolul 73 din Regulamentul privind ETIAS] și [articolul 54 din Regulamentul privind SIS în domeniul verificărilor la frontiere], separate în mod logic. Datele din CRRS nu permit identificarea persoanelor. Accesul la registru se acordă în mod securizat prin serviciile transeuropene securizate de telematică între administrații (TESTA), cu un control al accesului și profiluri de utilizator specifice, exclusiv în scopul întocmirii de rapoarte și statistici, autorităților menționate la [articolul 63 din Regulamentul privind EES], articolul 17 din Regulamentul (CE) nr. 767/2008, [articolul 73 din Regulamentul privind ETIAS] și [articolul 54 din Regulamentul privind SIS în domeniul verificărilor la frontiere].

3. Agenția eu-LISA anonimizează datele și înregistrează aceste date anonimizate în CRRS. Procesul de anonimizare a datelor este automatizat.

4. CRRS este alcătuit din următoarele componente:

   (a) o infrastructură centrală, constând într-un registru de date care permite anonimizarea datelor;

[75] Regulamentul (CE) nr. 168/2007 al Consiliului din 15 februarie 2007 privind înființarea Agenției pentru Drepturi Fundamentale a Uniunii Europene (JO L 53, 22.2.2007, p. 1).

(b) o infrastructură de comunicații securizată pentru a conecta CRRS la EES, [ETIAS], SIV și SIS, precum și la infrastructurile centrale ale BMS comun, CIR și MID.

5. Comisia stabilește, prin acte de punere în aplicare, norme detaliate privind funcționarea CRRS, inclusiv garanții specifice pentru prelucrarea datelor cu caracter personal menționate la alineatele (2) și (3) și norme de securitate aplicabile registrului. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 64 alineatul (2).

CAPITOLUL VII
Protecția datelor

Articolul 40
Operatorul de date

1. În ceea ce privește prelucrarea datelor în serviciul comun de comparare a datelor biometrice (BMS comun), autoritățile statelor membre care sunt operatori pentru VIS, EES și, respectiv, SIS sunt considerate, de asemenea, operatori în conformitate cu articolul 4 alineatul (7) din Regulamentul (UE) 2016/679 în ceea ce privește modelele biometrice obținute din datele menționate la articolul 13 pe care acestea le introduc în sistemele respective și sunt responsabile de prelucrarea modelelor biometrice în BMS comun.

2. În ceea ce privește prelucrarea datelor în registrul comun de date de identitate (CIR), autoritățile statelor membre care sunt operatori pentru VIS, EES și, respectiv, [ETIAS] sunt considerate, de asemenea, operatori în conformitate cu articolul 4 alineatul (7) din Regulamentul (UE) 2016/679 în ceea ce privește datele menționate la articolul 18 pe care le introduc în sistemele respective și sunt responsabile de prelucrarea datelor cu caracter personal în CIR.

3. În ceea ce privește prelucrarea datelor în detectorul de identități multiple:

(a) Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă este considerată operator de date în conformitate cu articolul 2 litera (b) din Regulamentul (CE) nr. 45/2001 în ceea ce privește prelucrarea datelor cu caracter personal de către unitatea centrală a ETIAS;

(b) autoritățile statelor membre care introduc sau modifică date în dosarul de confirmare a identității sunt considerate, de asemenea, operatori în conformitate cu articolul 4 alineatul (7) din Regulamentul (UE) 2016/679 și sunt responsabile de prelucrarea datelor cu caracter personal în detectorul de identități multiple;

Articolul 41
Persoana împuternicită de către operatorul de date

În ceea ce privește prelucrarea datelor cu caracter personal în CIR, eu-LISA este considerată persoana împuternicită de către operatorul de date în conformitate cu articolul 2 litera (e) din Regulamentul (CE) nr. 45/2001.

Articolul 42
Securitatea prelucrărilor

1. Atât eu-LISA, cât și autoritățile din statele membre asigură securitatea prelucrărilor de date cu caracter personal efectuate în temeiul aplicării prezentului regulament. Agenția eu-

LISA, [unitatea centrală a ETIAS] și autoritățile din statele membre cooperează în ceea ce privește sarcinile legate de securitate.

2. Fără a aduce atingere articolului 22 din Regulamentul (CE) nr. 45/2001, eu-LISA ia măsurile necesare pentru a asigura securitatea componentelor de interoperabilitate și a infrastructurii de comunicații aferente.

3. Mai precis, eu-LISA adoptă măsurile necesare, în special un plan de securitate, un plan de asigurare a continuității activității și un plan de recuperare în caz de dezastru, pentru:

(a) a proteja fizic datele, inclusiv prin elaborarea de planuri de urgență în scopul protejării infrastructurii critice;

(b) a împiedica citirea, copierea, modificarea sau ștergerea neautorizate a suporturilor de date;

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

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

(e) a asigura faptul că persoanele autorizate să acceseze componentele de interoperabilitate au acces numai la datele care fac obiectul autorizației lor de acces, prin utilizarea exclusivă a unor nume de utilizator individuale și a unor moduri de acces confidențiale;

(f) 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 a datelor;

(g) a asigura faptul că se poate verifica și stabili ce date au fost prelucrate în componentele de interoperabilitate, în ce moment, de către cine și cu ce scop;

(h) a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transmiterii datelor cu caracter personal către sau din componentele de interoperabilitate sau în timpul transportului suporturilor de date, în special prin intermediul unor tehnici de criptare corespunzătoare;

(i) a monitoriza eficacitatea măsurilor de securitate prevăzute la prezentul alineat și a se lua măsurile de organizare necesare referitoare la supravegherea internă, astfel încât să se asigure respectarea dispozițiilor prezentului regulament.

4. Statele membre iau măsuri echivalente celor menționate la alineatul (3) în materie de securitate în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile care au drept de acces la oricare dintre componentele de interoperabilitate.

Articolul 43
Confidențialitatea datelor din SIS

1. Fiecare stat membru aplică propriile norme privind secretul profesional sau alte obligații echivalente de confidențialitate pentru toate persoanele și organismele care lucrează cu date din SIS accesate prin intermediul oricărei componente de interoperabilitate, în conformitate cu dreptul său național. Această obligație se aplică și după ce persoanele respective au încetat să mai ocupe o anumită funcție sau un anumit post.

2. Fără a aduce atingere articolului 17 din Statutul funcționarilor Uniunii Europene și Regimul aplicabil celorlalți agenți ai Uniunii Europene, eu-LISA aplică norme

corespunzătoare privind secretul profesional sau alte obligații echivalente de confidențialitate pentru toți membrii personalului său care lucrează cu date din SIS, la standarde comparabile cu cele prevăzute la alineatul (1). Obligația menționată se aplică și după ce persoanele respective au încetat să mai ocupe o anumită funcție sau un anumit post ori după ce și-au încetat activitatea.

Articolul 44
Incidentele de securitate

1. Orice eveniment care are sau poate avea un impact asupra securității componentelor de interoperabilitate 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 a fost sau este posibil să fi fost compromisă.

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

3. Fără a aduce atingere notificării și comunicării unei încălcări a securității datelor cu caracter personal în temeiul articolului 33 din Regulamentul (UE) 2016/679, al articolului 30 din Directiva (UE) 2016/680 sau al ambelor articole, statele membre notifică incidentele de securitate Comisiei, agenției eu-LISA și Autorității Europene pentru Protecția Datelor. În cazul unui incident de securitate legat de infrastructura centrală a componentelor de interoperabilitate, eu-LISA notifică Comisia și Autoritatea Europeană pentru Protecția Datelor.

4. Informațiile privind un incident de securitate care are sau poate avea un impact asupra funcționării componentelor de interoperabilitate sau asupra disponibilității, integrității și confidențialității datelor sunt puse la dispoziția statelor membre și se raportează în conformitate cu planul de gestionare a incidentelor întocmit de eu-LISA.

5. Statele membre în cauză și eu-LISA colaborează în cazul unui incident de securitate. Comisia stabilește detaliile acestei cooperări prin intermediul unor acte de punere în aplicare. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 64 alineatul (2).

Articolul 45
Automonitorizarea

Statele membre și organismele relevante ale UE se asigură că fiecare autoritate care are acces la componentele de interoperabilitate ia măsurile necesare pentru a monitoriza respectarea prezentului regulament și cooperează, dacă este cazul, cu autoritatea națională de supraveghere.

Operatorii de date menționați la articolul 40 iau măsurile necesare pentru a monitoriza respectarea dispozițiilor prezentului regulament pe parcursul prelucrării datelor, inclusiv prin verificarea frecventă a înregistrărilor, și cooperează, după caz, cu autoritățile de supraveghere menționate la articolele 49 și 50.

Articolul 46
Dreptul la informare

1. Fără a aduce atingere dreptului la informare prevăzut la articolele 11 și 12 din Regulamentul (CE) nr. 45/2001 și la articolele 13 și 14 din Regulamentul (UE) 2016/679, persoanele ale căror date sunt stocate în serviciul comun de comparare a datelor

biometrice, în registrul comun de date de identitate sau în detectorul de identități multiple sunt informate de către autoritatea care le colectează datele, la momentul colectării, cu privire la prelucrarea datelor cu caracter personal în sensul prezentului regulament, inclusiv cu privire la identitatea și datele de contact ale operatorilor de date respectivi, procedurile prin care își pot exercita drepturile de acces, de rectificare și de ștergere a acestora, precum și cu privire la datele de contact ale Autorității Europene pentru Protecția Datelor și ale autorității naționale de supraveghere din statul membru responsabil de colectarea datelor.

2. Persoanele ale căror date sunt înregistrate în EES, VIS sau [ETIAS] sunt informate cu privire la prelucrarea datelor în sensul prezentului regulament în conformitate cu alineatul (1) atunci când:

(a) [se creează sau se actualizează un dosar individual în EES în conformitate cu articolul 14 din Regulamentul privind EES];

(b) se creează sau se actualizează un dosar de cerere în VIS în conformitate cu articolul 8 din Regulamentul (CE) nr. 767/2008;

(c) [se creează sau se actualizează un dosar de cerere în ETIAS în conformitate cu articolul 17 din Regulamentul privind ETIAS;]

(d) – (nu se aplică);

(e) – (nu se aplică).

Articolul 47
Dreptul de acces, de rectificare și de ștergere

1. Pentru a-și exercita drepturile prevăzute la articolele 13, 14, 15 și 16 din Regulamentul (CE) nr. 45/2001 și la articolele 15, 16, 17 și 18 din Regulamentul (UE) 2016/679, orice persoană are dreptul de a depune o cerere în statul membru responsabil de verificarea manuală a identităților diferite sau în orice alt stat membru, care trebuie să o examineze și să răspundă.

2. Statul membru responsabil de verificarea manuală a identităților diferite, astfel cum se menționează la articolul 29, sau statul membru căruia i s-a adresat cererea răspunde în termen de 45 de zile de la primirea cererii.

3. În cazul în care o cerere de rectificare sau de ștergere a datelor cu caracter personal este adresată unui alt stat membru decât cel responsabil, statul membru căruia i s-a adresat cererea contactează autoritățile statului membru responsabil în termen de șapte zile, iar statul membru responsabil verifică exactitatea datelor și legalitatea prelucrării acestora în termen de 30 zile de la data la care a fost contactat.

4. În cazul în care, în urma examinării, se constată că datele stocate în detectorul de identități multiple (MID) conțin erori materiale sau au fost înregistrate în mod ilegal, statul membru responsabil sau, după caz, statul membru căruia i s-a adresat cererea rectifică sau șterge datele respective.

5. În cazul în care datele din MID se modifică de către statul membru responsabil în timpul perioadei lor de valabilitate, statul membru responsabil desfășoară activitățile de prelucrare prevăzute la articolul 27 și, după caz, la articolul 29 pentru a stabili dacă datele modificate trebuie conexate. În cazul în care, în urma prelucrării, nu se obține un rezultat pozitiv, statul membru responsabil sau, după caz, statul membru căruia i s-a adresat cererea șterge datele din dosarul de confirmare a identității. În cazul în care, în urma prelucrării automate, se obțin(e) unul sau mai multe rezultate pozitive, statul membru responsabil creează sau

actualizează conexiunea aferentă în conformitate cu dispozițiile relevante din prezentul regulament.

6. În cazul în care statul membru responsabil sau, după caz, statul membru căruia i s-a adresat cererea nu este de acord că datele înregistrate în MID conțin erori materiale sau că au fost înregistrate în mod ilegal, acesta adoptă o decizie administrativă prin care persoanei interesate i se explică în scris și fără întârziere motivele pentru care statul membru respectiv nu este dispus să rectifice sau să șteargă datele care o privesc.

7. În această decizie i se furnizează persoanei vizate și informații privind posibilitatea de a contesta decizia luată în privința cererii menționate la alineatul (3) și, dacă este cazul, informații cu privire la modalitatea de a introduce o acțiune sau de a depune o plângere la autoritățile sau instanțele judecătorești competente și cu privire la orice asistență de care poate beneficia, inclusiv din partea autorităților naționale de supraveghere competente.

8. Cererile înaintate în temeiul alineatului (3) conțin informațiile necesare pentru a identifica persoana vizată. Aceste informații se utilizează exclusiv pentru a permite exercitarea drepturilor menționate la alineatul (3) și apoi se șterg imediat.

9. Statul membru responsabil sau, după caz, statul membru căruia i s-a adresat cererea ține o evidență sub forma unui document scris care să ateste că s-a depus o cerere de tipul celei menționate la alineatul (3) și modul în care a fost soluționată aceasta și pune documentul respectiv, fără întârziere, la dispoziția autorităților naționale competente în materie de supraveghere a protecției datelor.

Articolul 48
Comunicarea datelor cu caracter personal către țări terțe, organizații internaționale și părți private

Datele cu caracter personal stocate în componentele de interoperabilitate sau accesate prin intermediul acestora nu se transferă și nu se pun la dispoziția unei țări terțe, a unei organizații internaționale sau a unei părți private, cu excepția transferurilor către Interpol în scopul efectuării prelucrării automate menționate la [articolul 18 alineatul (2) literele (b) și (m) din Regulamentul privind ETIAS] sau în sensul articolului 8 alineatul (2) din Regulamentul (UE) 2016/399. Aceste transferuri de date cu caracter personal către Interpol respectă articolul 9 din Regulamentul (CE) nr. 45/2001 și capitolul V din Regulamentul (UE) 2016/679.

Articolul 49
Supravegherea de către autoritatea națională de supraveghere

1. Autoritatea sau autoritățile de supraveghere desemnate în temeiul articolului 49 din Regulamentul (UE) 2016/679 se asigură că, cel puțin o dată la patru ani, se efectuează un audit al operațiunilor de prelucrare a datelor de către autoritățile naționale responsabile, în conformitate cu standardele internaționale de audit relevante.

2. Statele membre se asigură că autoritatea lor de supraveghere are resurse suficiente pentru a îndeplini sarcinile care i-au fost încredințate în temeiul prezentului regulament.

Articolul 50
Supravegherea de către Autoritatea Europeană pentru Protecția Datelor

Autoritatea Europeană pentru Protecția Datelor garantează că, cel puțin o dată la patru ani, se realizează un audit al activităților de prelucrare a datelor cu caracter personal desfășurate de eu-LISA, în conformitate cu standardele internaționale de audit relevante. Un raport al acestui audit se

trimite Parlamentului European, Consiliului, agenției eu-LISA, Comisiei și statelor membre. Agenției eu-LISA i se oferă posibilitatea de a face observații înainte de adoptarea rapoartelor.

Articolul 51
Cooperarea dintre autoritățile naționale de supraveghere și Autoritatea Europeană pentru Protecția Datelor

1. Autoritatea Europeană pentru Protecția Datelor acționează în strânsă cooperare cu autoritățile naționale de supraveghere în ceea ce privește aspecte specifice care necesită o implicare la nivel național, în special dacă Autoritatea Europeană pentru Protecția Datelor sau o autoritate națională de supraveghere identifică discrepanțe majore între practicile statelor membre sau transferuri potențial ilegale efectuate prin canalele de comunicare ale componentelor de interoperabilitate sau în contextul întrebărilor adresate de una sau mai multe autorități naționale de supraveghere cu privire la punerea în aplicare și interpretarea prezentului regulament.

2. În cazurile menționate la alineatul (1), supravegherea coordonată este asigurată în conformitate cu articolul 62 din Regulamentul (UE) XXXX/2018 [Regulamentul 45/2001 revizuit].

CAPITOLUL VIII
Responsabilități

Articolul 52
Responsabilitățile eu-LISA în timpul etapei de concepere și dezvoltare

1. Agenția eu-LISA se asigură că infrastructurile centrale ale componentelor de interoperabilitate sunt exploatate în conformitate cu prezentul regulament.

2. Componentele de interoperabilitate sunt găzduite de eu-LISA în siturile sale tehnice și asigură funcționalitățile prevăzute în prezentul regulament, în conformitate cu condițiile de securitate, disponibilitate, calitate și viteză prevăzute la articolul 53 alineatul (1).

3. Agenția eu-LISA este responsabilă de dezvoltarea componentelor de interoperabilitate, de orice adaptare necesară pentru asigurarea interoperabilității între sistemele centrale ale EES, VIS, [ETIAS], SIS, Eurodac și [ECRIS-TCN] și portalul european de căutare, serviciul comun de comparare a datelor biometrice, registrul comun de date de identitate și detectorul de identități multiple.

   Agenția eu-LISA definește modul în care este concepută arhitectura fizică a componentelor de interoperabilitate, inclusiv infrastructurile acestora de comunicații, precum și specificațiile tehnice și evoluția acestora în ceea ce privește infrastructura centrală și infrastructura de comunicații securizată, care sunt adoptate de către Consiliul de administrație, sub rezerva unui aviz favorabil din partea Comisiei. De asemenea, eu-LISA pune în aplicare orice adaptare necesară a EES, [ETIAS], SIS sau VIS care rezultă din stabilirea interoperabilității și este prevăzută de prezentul regulament.

   Agenția eu-LISA dezvoltă și implementează componentele de interoperabilitate cât mai curând posibil după intrarea în vigoare a prezentului regulament și adoptarea de către Comisie a măsurilor prevăzute la articolul 8 alineatul (2), articolul 9 alineatul (7), articolul 28 alineatele (5) și (6), articolul 37 alineatul (4), articolul 38 alineatul (4), articolul 39 alineatul (5) și articolul 44 alineatul (5).

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

4. În cursul fazei de concepere și dezvoltare se instituie un consiliu de administrație al programului, alcătuit din maximum 10 membri. Dintre aceștia, șapte membri sunt numiți de Consiliul de administrație al eu-LISA din rândul membrilor săi sau al membrilor săi supleanți, un membru este președintele Grupului consultativ privind interoperabilitatea menționat la articolul 65, un membru care reprezintă eu-LISA este numit de directorul executiv al acesteia și un membru este numit de Comisie. Membrii numiți de către Consiliul de administrație al eu-LISA sunt aleși numai din statele membre pentru care instrumentele legislative ce reglementează dezvoltarea, instituirea, operarea și utilizarea tuturor sistemelor informatice la scară largă gestionate de eu-LISA prevăd obligații depline în temeiul dreptului Uniunii și care vor participa la componentele de interoperabilitate.

5. Consiliul de administrație al programului se întrunește periodic și cel puțin de trei ori pe trimestru. Acesta asigură gestionarea adecvată a etapei de concepere și dezvoltare a componentelor de interoperabilitate.

   Consiliul de administrație al programului prezintă lunar Consiliului de administrație rapoarte scrise privind evoluția proiectului. Consiliul de administrație al programului nu are competențe decizionale și nu dispune de un mandat de reprezentare a membrilor Consiliului de administrație al eu-LISA.

6. Consiliul de administrație al eu-LISA stabilește regulamentul de procedură al Consiliului de administrație al programului, care include în special norme privind:

   (a) președinția;

   (b) locul reuniunilor;

   (c) pregătirea reuniunilor;

   (d) accesul experților la reuniuni;

   (e) planurile de comunicare care asigură informarea completă a membrilor neparticipanți din cadrul Consiliului de administrație.

   Președinția este asigurată de un stat membru pentru care instrumentele legislative care reglementează dezvoltarea, instituirea, operarea și utilizarea tuturor sistemelor informatice la scară largă gestionate de eu-LISA prevăd obligații depline în temeiul dreptului Uniunii.

   Toate cheltuielile de deplasare și de ședere suportate de membrii Consiliului de administrație al programului sunt plătite de agenție, iar articolul 10 din regulamentul intern al eu-LISA se aplică *mutatis mutandis*. Agenția eu-LISA asigură secretariatul Consiliului de administrație al programului.

   Grupul consultativ privind interoperabilitatea menționat la articolul 65 se reunește periodic până la începerea funcționării componentelor de interoperabilitate. După fiecare reuniune, grupul consultativ prezintă un raport Consiliului de administrație al programului. Grupul consultativ furnizează expertiză tehnică pentru a asista Consiliul de administrație al programului în îndeplinirea sarcinilor sale și monitorizează stadiul de pregătire a statelor membre.

Articolul 53
Responsabilitățile eu-LISA după începerea funcționării

1. După începerea funcționării fiecărei componente de interoperabilitate, eu-LISA este responsabilă de gestionarea tehnică a infrastructurii centrale și a interfețelor uniforme

naționale. În cooperare cu statele membre, eu-LISA asigură în permanență cele mai bune tehnologii disponibile, sub rezerva unei analize costuri-beneficii. Agenția este, de asemenea, responsabilă de gestionarea tehnică a infrastructurii de comunicații menționate la articolele 6, 12, 17, 25 și 39.

Gestionarea tehnică a componentelor de interoperabilitate cuprinde toate sarcinile necesare pentru a menține în funcțiune componentele de interoperabilitate 24 de ore pe zi, 7 zile pe săptămână, în conformitate cu prezentul regulament, în special lucrările de întreținere și dezvoltările tehnice necesare pentru a se asigura funcționarea componentelor la un nivel satisfăcător de calitate tehnică, mai ales în ceea ce privește timpul de răspuns pentru efectuarea de căutări în infrastructurile centrale în conformitate cu specificațiile tehnice.

2. Fără a aduce atingere articolului 17 din Statutul funcționarilor Uniunii Europene, eu-LISA aplică norme corespunzătoare privind secretul profesional sau alte obligații echivalente de confidențialitate tuturor membrilor personalului său care lucrează 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.

3. Agenția eu-LISA dezvoltă și întreține un mecanism și proceduri de verificare a calității datelor stocate în serviciul comun de comparare a datelor biometrice și în registrul comun de date de identitate, în conformitate cu articolul 37.

4. Agenția eu-LISA îndeplinește, de asemenea, sarcini legate de asigurarea formării privind utilizarea tehnică a componentelor de interoperabilitate.

Articolul 54
Responsabilitățile statelor membre

1. Fiecare stat membru este responsabil de:

(a) conectarea la infrastructura de comunicare a portalului european de căutare (ESP) și a registrului comun de date de identitate (CIR);

(b) integrarea sistemelor și a infrastructurilor naționale existente cu ESP, serviciul comun de comparare a datelor biometrice, CIR și detectorul de identități multiple;

(c) organizarea, gestionarea, operarea și întreținerea infrastructurii naționale existente și de conectarea acesteia la componentele de interoperabilitate;

(d) gestionarea accesului și modalitățile de acces al personalului autorizat în mod corespunzător și al personalului împuternicit în mod corespunzător din cadrul autorităților naționale competente la ESP, CIR și detectorul de identități multiple în conformitate cu dispozițiile prezentului regulament, precum și de crearea și actualizarea periodică a unei liste a personalului menționat și a profilurilor acestora;

(e) adoptarea măsurilor legislative menționate la articolul 20 alineatul (3) pentru a avea acces la CIR în scopuri de identificare;

(f) verificarea manuală a identităților diferite, menționată la articolul 29;

(g) implementarea cerințelor de calitate a datelor în sistemele de informații ale UE și în componentele de interoperabilitate;

(h) remedierea oricăror deficiențe identificate în raportul de evaluare privind calitatea datelor efectuat de Comisie și menționat la articolul 37 alineatul (5).

2. Fiecare stat membru își conectează la CIR autoritățile desemnate menționate la articolul 4 alineatul (24).

Articolul 55
Responsabilitățile unității centrale a ETIAS

Unitatea centrală a ETIAS este responsabilă de:

(a) verificarea manuală a identităților diferite, menționată la articolul 29;

(b) efectuarea unei detectări de identități multiple în datele stocate în VIS, Eurodac și SIS, menționată la articolul 59.

CAPITOLUL IX
Modificări aduse altor instrumente ale Uniunii

Articolul 55a
Modificări aduse Regulamentului (UE) 2016/399

Regulamentul (UE) 2016/399 se modifică după cum urmează:

La articolul 8 din Regulamentul (UE) 2016/399, se adaugă următorul alineat (4a):

„(4a) În cazul în care, la intrare sau la ieșire, în urma consultării bazelor de date relevante, inclusiv a detectorului de identități multiple prin intermediul portalului european de căutare menționat la [articolul 4 punctul 36 și, respectiv, punctul 33 din Regulamentul 2018/XX privind interoperabilitatea], rezultă o conexiune galbenă sau se detectează o conexiune roșie, persoana care face obiectul controlului de identitate este supusă unei verificări în linia a doua.

Polițistul de frontieră din linia a doua consultă detectorul de identități multiple și registrul comun de date de identitate menționate la [articolul 4 alineatul (35) din Regulamentul 2018/XX privind interoperabilitatea] sau Sistemul de Informații Schengen ori ambele pentru a evalua diferențele dintre identitățile conexate și efectuează verificările suplimentare necesare pentru a lua o decizie privind statutul și culoarea conexiunii, precum și cu privire la intrarea sau refuzul intrării persoanei în cauză.

În conformitate cu [articolul 59 alineatul (1) din Regulamentul nr. 2018/XX], prezentul alineat se aplică numai de la începerea funcționării detectorului de identități multiple.”

Articolul 55b
Modificări aduse Regulamentului (UE) 2017/2226

Regulamentul (UE) 2017/2226 se modifică după cum urmează:

1) La articolul 1 se adaugă următorul alineat:

„(1a) Prin faptul că stochează date de identitate, documente de călătorie și date biometrice în registrul comun de date de identitate instituit prin [articolul 17 din Regulamentul 2018/XX privind interoperabilitatea], EES contribuie la facilitarea și acordarea de asistență în vederea identificării corecte a persoanelor înregistrate în EES în condițiile și pentru realizarea obiectivelor finale prevăzute la [articolul 20] din regulamentul menționat.”

2) La articolul 3 se adaugă următorul punct (21a):

„«CIR» înseamnă un registru comun de date de identitate, astfel cum este definit la [articolul 4 punctul 35 din Regulamentul 2018/XX privind interoperabilitatea];”

3) La articolul 3 alineatul (1), punctul (22) se înlocuiește cu următorul text:

„(22) «date din EES» înseamnă toate datele stocate în sistemul central al EES și în CIR, în conformitate cu articolul 14 și cu articolele 16-20.”

4) La articolul 3 se introduce un nou punct (22a):

„(22a) «date de identitate» înseamnă datele prevăzute la articolul 16 alineatul (1) litera (a);”

5) La articolul 6 alineatul (1) se introduce următoarea literă:

„(j) să asigure identificarea corectă a persoanelor.”

6) La articolul 7 alineatul (1), litera (a) se înlocuiește cu următorul text:

„(a) registrul comun de date de identitate (CIR), astfel cum este menționat la [articolul 17 alineatul (2) litera (a) din Regulamentul 2018/XX privind interoperabilitatea];

(aa) un sistem central (sistemul central al EES);”

7) La articolul 7 alineatul (1), litera (f) se înlocuiește cu următorul text:

„(f) o infrastructură de comunicații securizată între sistemul central al EES și infrastructurile centrale ale portalului european de căutare instituit prin [articolul 6 din Regulamentul 2018/XX privind interoperabilitatea], serviciul comun de comparare a datelor biometrice instituit prin [articolul 12 din Regulamentul 2018/XX privind interoperabilitatea], registrul comun de date de identitate, instituit prin [articolul 17 din Regulamentul 2018/XX privind interoperabilitatea] și detectorul de identități multiple instituit prin [articolul 25 din Regulamentul 2018/XX privind interoperabilitatea].”

8) La articolul 7 se adaugă următorul alineat:

„(1a) CIR conține datele menționate la articolul 16 alineatul (1) literele (a)-(d) și la articolul 17 alineatul (1) literele (a)-(c), iar restul de date din EES sunt stocate în sistemul central al EES.”

9) La articolul 9 se adaugă următorul alineat:

„(3) Accesul la consultarea datelor din EES stocate în CIR este rezervat exclusiv personalului autorizat în mod corespunzător din cadrul autorităților competente ale statelor membre și personalului autorizat în mod corespunzător din cadrul organismelor UE cu competențe în scopurile prevăzute la [articolele 20 și 21 din Regulamentul 2018/XX privind interoperabilitatea]. Accesul este limitat la ceea ce este necesar pentru îndeplinirea sarcinilor de către aceste autorități naționale și organisme ale UE, în conformitate cu scopurile menționate, și este proporțional cu obiectivele urmărite.”

10) La articolul 21 alineatul (1), cuvintele „sistemul central al EES” și „sistemului central al EES” se înlocuiesc cu „sistemul central al EES sau CIR”.

11) La articolul 21 alineatul (2), cuvintele „în sistemul central al EES și în NUI” se înlocuiesc cu „în sistemul central al EES și în CIR, pe de o parte, și în NUI, pe de altă parte”.

12) La articolul 21 alineatul (2), cuvintele „sunt introduse în sistemul central al EES” se înlocuiesc cu cuvintele „sunt introduse în sistemul central al EES și în CIR”.

13) La articolul 32 se adaugă un nou alineat (1a):

„(1a) În cazul în care autoritățile desemnate au lansat o interogare în CIR în conformitate cu [articolul 22 din Regulamentul 2018/XX privind interoperabilitatea], acestea pot accesa EES pentru consultare în cazul în care din răspunsul primit, astfel cum se menționează la [articolul 22 alineatul (3) din Regulamentul 2018/XX privind interoperabilitatea], rezultă că datele sunt stocate în EES.”

14) Articolul 32 alineatul (2) se înlocuiește cu următorul text:

„(2) Accesul la EES ca instrument de identificare a unei persoane necunoscute despre care se crede că ar fi suspectul, autorul sau victima prezumată a unei infracțiuni de terorism sau a

unei alte infracțiuni grave este permis numai atunci când se lansează în CIR o interogare în conformitate cu [articolul 22 din Regulamentul 2018/XX privind interoperabilitatea] și sunt îndeplinite toate condițiile enumerate la alineatele (1) și (1a).

Această condiție suplimentară nu se aplică însă într-o situație de urgență, atunci când trebuie să se prevină un pericol iminent la adresa vieții unei persoane asociate cu o infracțiune de terorism sau cu o altă infracțiune gravă. Aceste motive întemeiate se includ în solicitarea electronică sau pe suport de hârtie pe care unitatea operațională a autorității desemnate o trimite punctului central de acces."

15) Articolul 32 alineatul (4) se elimină.

16) La articolul 33 se adaugă un nou alineat (1a):

„(1a) În cazul în care Europol a lansat o interogare în CIR în conformitate cu [articolul 22 din Regulamentul 2018/XX privind interoperabilitatea], acesta poate accesa EES pentru consultare în cazul în care din răspunsul primit, astfel cum se menționează la [articolul 22 alineatul (3) din Regulamentul 2018/XX privind interoperabilitatea], rezultă că datele sunt stocate în EES."

17) La articolul 33, alineatul (3) se înlocuiește cu următorul text:

„Condițiile prevăzute la articolul 32 alineatele (3)-(5) se aplică în consecință."

18) La articolul 34 alineatele (1) și (2), cuvintele „în sistemul central al EES" se înlocuiesc cu cuvintele „în CIR și, respectiv, în sistemul central al EES".

19) La articolul 34 alineatul (5), cuvintele „din sistemul central al EES" se înlocuiesc cu cuvintele „din sistemul central al EES și din CIR".

20) La articolul 35, alineatul (7) se înlocuiește cu următorul text:

„Sistemul central al EES și CIR informează de îndată toate statele membre cu privire la ștergerea datelor din EES sau CIR și, după caz, le elimină din lista persoanelor identificate menționată la articolul 12 alineatul (3)."

21) La articolul 36, cuvintele „a sistemului central al EES" se înlocuiesc cu cuvintele „a sistemului central al EES și a CIR".

22) La articolul 37 alineatul (1), cuvintele „dezvoltarea sistemului central al EES" se înlocuiesc cu „dezvoltarea sistemului central al EES și a CIR".

23) La articolul 37 alineatul (3) prima teză, cuvintele „a sistemului central al EES" și „pentru sistemul central al EES" se înlocuiesc cu „a sistemului central al EES și a CIR" și, respectiv, „pentru sistemul central al EES și pentru CIR".

24) La articolul 46 alineatul (1), se adaugă următoarea literă (f):

„(f) după caz, o mențiune privind utilizarea portalului european de căutare pentru a efectua interogări în EES, astfel cum se menționează la [articolul 7 alineatul (2) din Regulamentul (UE) nr. 2018/XX privind interoperabilitatea]."

25) Articolul 63 alineatul (2) se înlocuiește cu următorul text:

„(2) În sensul alineatului (1), eu-LISA stochează datele menționate la alineatul (1) în registrul central de raportare și statistici menționat la [articolul 39 din Regulamentul 2018/XX privind interoperabilitatea]."

26) La articolul 63 alineatul (4) se adaugă un paragraf nou:

„Statisticile zilnice sunt stocate în registrul central de raportare și statistici."

Articolul 55c
Modificări aduse Deciziei 2004/512/CE a Consiliului

Decizia 2004/512/CE a Consiliului de instituire a Sistemului de Informații privind Vizele (VIS) se modifică după cum urmează:

Articolul 1 alineatul (2) se modifică după cum urmează:

„(2) Sistemul de Informații privind Vizele se bazează pe o arhitectură centralizată și cuprinde:

(a) un registru comun de date de identitate (CIR), astfel cum se menționează la [articolul 17 alineatul (2) litera (a) din Regulamentul 2018/XX privind interoperabilitatea];

(b) un sistem central de informații, denumit în continuare «Sistemul Central de Informații privind Vizele» (CS-VIS);

(c) o interfață în fiecare stat membru, denumită în continuare «interfața națională» (NI-VIS), care asigură conectarea la autoritatea centrală națională relevantă din statul membru respectiv;

(d) o infrastructură de comunicații între Sistemul Central de Informații privind Vizele și interfețele naționale;

(e) un canal de comunicații securizat între sistemul central al EES și CS-VIS;

(f) o infrastructură de comunicații securizată între sistemul central al VIS și infrastructurile centrale ale portalului european de căutare instituit prin [articolul 6 din Regulamentul 2018/XX privind interoperabilitatea], serviciul comun de comparare a datelor biometrice instituit prin [articolul 12 din Regulamentul 2018/XX privind interoperabilitatea], registrul comun de date de identitate și detectorul de identități multiple (MID) instituit prin [articolul 25 din Regulamentul 2018/XX privind interoperabilitatea]”.

Articolul 55d
Modificări aduse Regulamentului (CE) 767/2008

1) La articolul 1 se adaugă următorul alineat:

„(2) Prin faptul că stochează date de identitate, documente de călătorie și date biometrice în registrul comun de date de identitate (CIR) instituit prin [articolul 17 din Regulamentul 2018/XX privind interoperabilitatea], VIS contribuie la facilitarea și asistarea identificării corecte a persoanelor înregistrate în VIS în condițiile și pentru realizarea obiectivelor finale prevăzute la alineatul (1) al prezentului articol.”

2) La articolul 4, se adaugă următoarele puncte:

„(12) «date din VIS» înseamnă toate datele stocate în sistemul central VIS și în CIR în conformitate cu articolele 9-14.

(13) «date de identitate» înseamnă datele prevăzute la articolul 9 alineatul (4) literele (a)-(aa);

(14) «date dactiloscopice» înseamnă datele privind cele cinci amprente digitale ale indexului, degetului mijlociu, degetului inelar, degetului mic și degetului mare de la mâna dreaptă, FR: dacă acest lucru este posibil din punct de vedere fizic, și de la mâna stângă;

(15) «imagine facială» înseamnă imagini digitale ale feței;

(16) «date biometrice» înseamnă datele dactiloscopice și imaginea facială;”

3) La articolul 5 se adaugă următorul alineat:

„(1a) CIR conține datele menționate la articolul 9 alineatul (4) literele (a)-(cc) și la articolul 9 alineatele (5) și (6), celelalte date din VIS fiind stocate în sistemul central al VIS.”

4) Articolul 6 alineatul (2) se modifică după cum urmează:

„(2) Accesul la VIS pentru consultarea datelor este rezervat în mod exclusiv personalului autorizat în mod corespunzător din cadrul autorităților naționale ale fiecărui stat membru care are competențe în ceea ce privește scopurile prevăzute la articolele 15-22, și personalului autorizat în mod corespunzător din cadrul autorităților naționale ale fiecărui stat membru și al organismelor UE care are competențe în ceea ce privește scopurile prevăzute la [articolele 20 și 21 din Regulamentul 2018/XX privind interoperabilitatea], limitat la ceea ce este necesar pentru îndeplinirea sarcinilor care îi revin în conformitate cu aceste scopuri și proporțional cu obiectivele urmărite.”

5) Articolul 9 alineatul (4) literele (a)-(c) se modifică după cum urmează:

„(a) numele de familie, prenumele (numele de botez), data nașterii, cetățenia sau cetățeniile, sexul;

(aa) nume, numele la naștere (numele deținute anterior), locul și țara nașterii, cetățenia la naștere;

(b) tipul și numărul documentului sau documentelor de călătorie și codul din trei litere al țării emitente a documentului sau documentelor de călătorie;

(c) data expirării perioadei de valabilitate a documentului de călătorie;

(cc) autoritatea care a eliberat documentul de călătorie și data eliberării;”

6) Articolul 9 alineatul (5) se înlocuiește cu următorul text:

„imaginea facială, astfel cum este definită la articolul 4 punctul 15”.

7) La articolul 29 alineatul (2) litera (a), cuvântul „VIS” se înlocuiește cu „VIS sau CIR” în cele două cazuri în care apare.

Articolul 55e
Modificări aduse Deciziei 2008/633/JAI a Consiliului.

1) La articolul 5 se adaugă un nou alineat (1a):

„(1a) În cazul în care autoritățile desemnate au lansat o interogare în CIR în conformitate cu [articolul 22 din Regulamentul 2018/XX privind interoperabilitatea], acestea pot accesa VIS pentru consultare în cazul în care, din răspunsul primit, astfel cum se menționează la [articolul 22 alineatul (3) din Regulamentul 2018/XX privind interoperabilitatea], rezultă că datele sunt stocate în VIS.”

2) La articolul 7 se adaugă un nou alineat (1a):

„(1a) În cazul în care Europol a lansat o interogare în CIR în conformitate cu [articolul 22 din Regulamentul 2018/XX privind interoperabilitatea], acesta poate accesa VIS pentru consultare în cazul în care, din răspunsul primit, astfel cum se menționează la [articolul 22 alineatul (3) din Regulamentul 2018/XX privind interoperabilitatea], rezultă că datele sunt stocate în VIS.”

CAPITOLUL X
Dispoziții finale

Articolul 56
Întocmirea de rapoarte și de statistici

1. Personalul autorizat în mod corespunzător din cadrul autorităților competente ale statelor membre, din cadrul Comisiei și al agenției eu-LISA are acces pentru a consulta următoarele date referitoare la portalul european de căutare (ESP), exclusiv în scopul întocmirii de rapoarte și statistici, fără a permite identificarea individuală:

   (a) numărul de interogări pe utilizator de profil ESP;

   (b) numărul de interogări pentru fiecare bază de date a Interpol.

2. Personalul autorizat în mod corespunzător din cadrul autorităților competente ale statelor membre, din cadrul Comisiei și al agenției eu-LISA are acces pentru a consulta următoarele date referitoare la registrul comun de date de identitate, exclusiv în scopul întocmirii de rapoarte și statistici, fără a permite identificarea individuală:

   (a) numărul de interogări lansate în sensul articolelor 20, 21 și 22;

   (b) cetățenia, sexul și anul nașterii persoanei;

   (c) tipul documentului de călătorie, inclusiv codul din trei litere al țării emitente;

   (d) numărul de căutări efectuate cu și fără date biometrice.

3. Personalul autorizat în mod corespunzător din cadrul autorităților competente ale statelor membre, din cadrul Comisiei și al agenției eu-LISA are acces pentru a consulta următoarele date referitoare la detectorul de identități multiple, exclusiv în scopul întocmirii de rapoarte și statistici, fără a permite identificarea individuală:

   (a) cetățenia, sexul și anul nașterii persoanei;

   (b) tipul documentului de călătorie, inclusiv codul din trei litere al țării emitente;

   (c) numărul de căutări efectuate cu și fără date biometrice;

   (d) numărul de conexiuni stabilite, în funcție de tip.

4. Personalul autorizat în mod corespunzător din cadrul Agenției Europene pentru Poliția de Frontieră și Garda de Coastă, instituită prin Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului[76], are acces pentru a consulta datele menționate la alineatele (1), (2) și (3) în scopul de a efectua analize de risc și evaluări ale vulnerabilității, astfel cum se prevede la articolele 11 și 13 din respectivul regulament.

5. În sensul alineatului (1), eu-LISA stochează datele menționate la alineatul (1) în registrul central de raportare și statistici menționat în capitolul VII din prezentul regulament. Datele incluse în registru nu permit identificarea persoanelor fizice, dar permit autorităților enumerate la alineatul (1) să obțină rapoarte și statistici adaptabile pentru a spori eficiența verificărilor la frontieră, a sprijini autoritățile să prelucreze cererile de viză și a sprijini elaborarea de politici bazate pe date concrete în materie de migrație și de securitate în Uniune.

[76] Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului din 14 septembrie 2016 privind Poliția de frontieră și garda de coastă la nivel european și de modificare a Regulamentului (UE) 2016/399 al Parlamentului European și al Consiliului și de abrogare a Regulamentului (CE) nr. 863/2007 al Parlamentului European și al Consiliului, a Regulamentului (CE) nr. 2007/2004 al Consiliului și a Deciziei 2005/267/CE a Consiliului (JO L 251, 16.9.2016, p. 1).

Articolul 57
Perioada de tranziție pentru utilizarea portalului european de căutare

Pentru o perioadă de doi ani de la data la care începe funcționarea ESP, obligațiile menționate la articolul 7 alineatele (2) și (4) nu se aplică, iar utilizarea ESP este opțională.

Articolul 58
Perioada de tranziție aplicabilă dispozițiilor privind accesul la registrul comun de date de identitate în scopul asigurării respectării legii

Articolul 22, articolul 55b alineatele (13), (14), (15) și (16), precum și articolul 55e se aplică de la data de începere a funcționării componentelor, menționată la articolul 62 alineatul (1).

Articolul 59
Perioada de tranziție aplicabilă detectorului de identități multiple

1. În termen de un an de la notificarea de către eu-LISA a încheierii perioadei de testare a detectorului de identități multiple (MID) prevăzute la articolul 62 alineatul (1) litera (b) și înainte de începerea funcționării MID, unitatea centrală a ETIAS, astfel cum este menționată la [articolul 33 litera (a) din Regulamentul (UE) 2016/1624], este responsabilă de efectuarea unei detectări de identități multiple între datele stocate în VIS, Eurodac și SIS. Detectarea identităților multiple se efectuează folosind exclusiv date biometrice, în conformitate cu articolul 27 alineatul (2) din prezentul regulament.

2. În cazul în care, în urma interogărilor, se obține(e) unul sau mai multe rezultate pozitive și datele de identitate ale dosarelor astfel conexate sunt identice sau similare, se stabilește o conexiune albă în conformitate cu articolul 33.

   În cazul în care, în urma interogărilor, se obține(e) unul sau mai multe rezultate pozitive și datele de identitate ale dosarelor astfel conexate nu pot fi considerate similare, se stabilește o conexiune galbenă în conformitate cu articolul 30 și se aplică procedura prevăzută la articolul 29.

   În cazul în care se obțin mai multe rezultate pozitive, se stabilește o conexiune pentru fiecare componentă a datelor care a generat rezultatul pozitiv.

3. În cazul în care se stabilește o conexiune galbenă, MID acordă acces unității centrale a ETIAS la datele de identitate existente în diferitele sisteme de informații.

4. În cazul în care se stabilește o conexiune cu o semnalare din SIS, alta decât o semnalare privind refuzul intrării sau o semnalare privind un document de călătorie declarat pierdut, furat sau anulat în conformitate cu articolul 24 din Regulamentul privind SIS în domeniul verificărilor la frontiere și, respectiv, cu articolul 38 din Regulamentul privind SIS în domeniul asigurării respectării legii, MID acordă acces biroului SIRENE din statul membru care a creat semnalarea la datele de identitate existente în diferitele sisteme de informații.

5. Unitatea centrală a ETIAS sau biroul SIRENE din statul membru care a creat semnalarea are acces la datele conținute în dosarul de confirmare a identității, analizează identitățile diferite și actualizează conexiunea în conformitate cu articolele 31, 32 și 33, adăugând-o la dosarul de confirmare a identității.

6. În cazul în care este necesar, eu-LISA acordă asistență unității centrale a ETIAS în vederea detectării identităților multiple menționată în prezentul articol.

Articolul 60
Costuri

(1) Costurile aferente instituirii și funcționării ESP, a serviciului comun de comparare a datelor biometrice, a registrului comun de date de identitate (CIR) și a MID sunt suportate din bugetul general al Uniunii.

(2) Costurile aferente integrării infrastructurilor naționale existente și a conectării lor la interfețele uniforme naționale, precum și cele aferente găzduirii interfețelor uniforme naționale sunt suportate din bugetul general al Uniunii Europene.

Sunt excluse următoarele costuri:

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

(b) costurile aferente găzduirii sistemelor IT naționale (spații, implementare, electricitate, răcire);

(c) costurile aferente operării sistemelor IT naționale (operatori și contracte de sprijin);

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

(3) Costurile aferente autorităților desemnate menționate la articolul 4 alineatul (24) sunt suportate de către fiecare stat membru și, respectiv, de către Europol. Costurile aferente conectării autorităților desemnate la CIR sunt suportate de către fiecare stat membru și, respectiv, de către Europol.

Articolul 61
Notificări

1. Statele membre notifică agenției eu-LISA autoritățile menționate la articolele 7, 20, 21 și 26 care pot utiliza sau avea acces la ESP, CIR și, respectiv, MID.

O listă consolidată a acestor autorități se publică în *Jurnalul Oficial al Uniunii Europene* în termen de trei luni de la data începerii funcționării fiecărei componente de interoperabilitate în conformitate cu articolul 62. În cazul în care lista este modificată, eu-LISA publică o actualizare consolidată a acesteia o dată pe an.

2. Agenția eu-LISA notifică Comisiei finalizarea cu succes a testării menționate la articolul 62 alineatul (1) litera (b).

3. Unitatea centrală a ETIAS notifică Comisiei finalizarea cu succes a măsurii tranzitorii prevăzute la articolul 59.

4. Comisia pune la dispoziția statelor membre și a publicului, prin intermediul unui site web public actualizat în permanență, informațiile notificate în temeiul alineatului (1).

Articolul 62
Începerea funcționării

1. Comisia stabilește data de la care fiecare componentă de interoperabilitate începe să funcționeze, după ce sunt îndeplinite următoarele condiții:

(a) au fost luate măsurile menționate la articolul 8 alineatul (2), articolul 9 alineatul (7), articolul 28 alineatele (5) și (6), articolul 37 alineatul (4), articolul 38 alineatul (4), articolul 39 alineatul (5) și articolul 44 alineatul (5);

(b) eu-LISA a notificat finalizarea cu succes a unei testări complete a componentelor de interoperabilitate relevante, care trebuie efectuată de către eu-LISA în cooperare cu statele membre;

(c) eu-LISA a validat modalitățile tehnice și juridice de colectare și transmitere a datelor menționate la articolele 8 alineatul (1), 13, 19, 34 și 39 și a notificat aceste modalități Comisiei;

(d) statele membre au trimis Comisiei notificarea menționată la articolul 61 alineatul (1);

(e) unitatea centrală a ETIAS a trimis Comisiei notificarea menționată la articolul 61 alineatul (3) în ceea ce privește detectorul de identități multiple.

2. Comisia informează Parlamentul European și Consiliul cu privire la rezultatele testării realizate în temeiul alineatului (1) litera (b).

3. Decizia Comisiei menționată la alineatul (1) se publică în *Jurnalul Oficial al Uniunii Europene*.

4. Statele membre și Europol încep să utilizeze componentele de interoperabilitate de la data stabilită de Comisie în conformitate cu alineatul (1).

Articolul 63
Exercitarea delegării de competențe

1. Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.

2. Competența de a adopta actele delegate menționate la articolul 8 alineatul (2) și la articolul 9 alineatul (7) este conferită Comisiei pentru o perioadă de timp nedeterminată de la [*data intrării în vigoare a prezentului regulament*].

3. Delegarea de competențe menționată la articolul 8 alineatul (2) și la articolul 9 alineatul (7) poate fi revocată oricând de Parlamentul European sau de Consiliu. Prin decizia de revocare ia sfârșit delegarea competențelor specificată în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau la o dată ulterioară menționată în decizie. Decizia nu aduce atingere valabilității actelor delegate care sunt deja în vigoare.

4. Înainte de adoptarea unui act delegat, Comisia îi consultă pe experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional privind o mai bună legiferare din 13 aprilie 2016.

5. De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

6. Actul delegat adoptat în temeiul articolului 8 alineatul (2) și al articolului 9 alineatul (7) intră în vigoare numai în cazul în care Parlamentul European sau Consiliul nu a formulat nicio obiecție în termen de [două luni] de la notificarea actului respectiv Parlamentului European și Consiliului sau dacă, înainte de expirarea acestui termen, atât Parlamentul European, cât și Consiliul au informat Comisia că nu vor formula obiecții. Termenul în cauză se prelungește cu [două luni] la inițiativa Parlamentului European sau a Consiliului.

Articolul 64
Procedura comitetului

1. Comisia este asistată de un comitet. Comitetul respectiv este un comitet în sensul Regulamentului (UE) nr. 182/2011.

2. Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

Articolul 65
Grupul consultativ

Agenția eu-LISA instituie un grup consultativ care îi furnizează cunoștințe de specialitate referitoare la interoperabilitate, în special în contextul pregătirii programului său anual de lucru și a raportului său anual de activitate. În faza de concepere și dezvoltare a instrumentelor de interoperabilitate, se aplică articolul 52 alineatele (4) și (6).

Articolul 66
Formare

Agenția eu-LISA îndeplinește atribuții legate de furnizarea de cursuri de formare privind utilizarea tehnică a componentelor de interoperabilitate în conformitate cu Regulamentul (UE) nr. 1077/2011.

Articolul 67
Manual practic

Comisia, în strânsă cooperare cu statele membre, cu eu-LISA și cu alte agenții relevante, pune la dispoziție un manual practic pentru implementarea și gestionarea componentelor de interoperabilitate. Manualul practic furnizează orientări, recomandări și bune practici de natură tehnică și operațională. Comisia adoptă manualul sub forma unei recomandări.

Articolul 68
Monitorizare și evaluare

1. Agenția eu-LISA se asigură că există proceduri pentru a monitoriza dezvoltarea componentelor de interoperabilitate din perspectiva obiectivelor legate de planificare și costuri și pentru a monitoriza funcționarea componentelor de interoperabilitate din perspectiva obiectivelor legate de rezultatele tehnice, eficacitatea costurilor, securitate și calitatea serviciilor.

2. În termen de [*șase luni de la data intrării în vigoare a prezentului regulament*] și, ulterior, la fiecare șase luni în etapa de dezvoltare a componentelor de interoperabilitate, eu-LISA prezintă un raport Parlamentului European și Consiliului privind situația dezvoltării componentelor de interoperabilitate. După încheierea fazei de dezvoltare, se transmite Parlamentului European și Consiliului un raport în care se explică în detaliu modul în care au fost îndeplinite obiectivele, în special obiectivele legate de planificare și costuri, și în care se justifică eventualele abateri.

3. În scopul întreținerii tehnice, eu-LISA are acces la informațiile necesare legate de operațiunile de prelucrare a datelor efectuate în componentele de interoperabilitate.

4. După patru ani de la începerea funcționării fiecărei componente de interoperabilitate și, ulterior, o dată la patru ani, eu-LISA prezintă Parlamentului European, Consiliului și

Comisiei un raport privind funcționarea tehnică a componentelor de interoperabilitate, inclusiv în ceea ce privește securitatea acestora.

5. În plus, la un an după fiecare raport prezentat de eu-LISA, Comisia realizează o evaluare generală a componentelor, inclusiv:

(a) o analiză a aplicării prezentului regulament;

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

(c) o analiză a valabilității în continuare a raționamentului care stă la baza componentelor de interoperabilitate;

(d) o evaluare a securității componentelor de interoperabilitate;

(e) o evaluare a eventualelor implicații, inclusiv a impactului disproporționat asupra fluidității traficului la punctele de trecere a frontierelor și a implicațiilor cu un impact bugetar asupra bugetului Uniunii.

Evaluările cuprind orice recomandări necesare. Comisia transmite raportul de evaluare Parlamentului European, Consiliului, Autorității Europene pentru Protecția Datelor și Agenției pentru Drepturi Fundamentale a Uniunii Europene instituită prin Regulamentul (CE) nr. 168/2007 al Consiliului[77].

6. Statele membre și Europolul furnizează agenției eu-LISA și Comisiei informațiile necesare pentru redactarea rapoartelor menționate la alineatele (4) și (5). Aceste informații nu trebuie să pericliteze metodele de lucru și nu includ informații care să dezvăluie sursele, membrii personalului sau investigațiile autorităților desemnate.

7. Agenția eu-LISA furnizează Comisiei informațiile necesare pentru realizarea evaluărilor generale menționate la alineatul (5).

8. Respectând dispozițiile dreptului național referitoare la publicarea informațiilor sensibile, fiecare stat membru și Europol întocmesc rapoarte anuale privind eficacitatea accesului la datele stocate în registrul comun de date de identitate în scopul asigurării respectării legii, care conțin informații și statistici privind:

(a) scopul exact al consultării, inclusiv tipul infracțiunii de terorism sau al altei infracțiuni grave;

(b) motivele întemeiate invocate în sprijinul suspiciunii justificate că suspectul, autorul sau victima intră sub incidența [Regulamentului privind EES], a Regulamentului privind VIS sau [a Regulamentului privind ETIAS];

(c) numărul solicitărilor de acces la registrul comun de date de identitate în scopul asigurării respectării legii;

(d) numărul și tipul de cazuri finalizate cu identificări reușite;

(e) necesitatea și utilizarea prevederii privind situația excepțională de urgență, precum și cazurile în care urgența respectivă nu a fost acceptată în urma verificării *ex-post* efectuate de punctul central de acces.

Rapoartele anuale ale statelor membre și ale Europol se transmit Comisiei până la data de 30 iunie a anului următor.

[77] Regulamentul (CE) nr. 168/2007 al Consiliului din 15 februarie 2007 privind înființarea Agenției pentru Drepturi Fundamentale a Uniunii Europene (JO L 53, 22.2.2007, p. 1).

Articolul 69
Intrarea în vigoare și aplicabilitatea

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

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

Adoptat la Strasbourg,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președintele	*Președintele*

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Denumirea propunerii/inițiativei

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

1.3. Tipul propunerii/inițiativei

1.4. Obiectiv(e)

1.5. Motivele propunerii/inițiativei

1.6. Durata și impactul financiar

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

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

2.2. Sistemul de gestiune și de control

2.3. Măsuri de prevenire a fraudelor și a neregulilor

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

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

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

3.2.2. Impactul estimat asupra creditelor operaționale

3.2.3. Impactul estimat asupra creditelor cu caracter administrativ

3.2.4. Compatibilitatea cu actualul cadru financiar multianual

3.2.5. Contribuția terților

3.3. Impactul estimat asupra veniturilor

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Denumirea propunerii/inițiativei

Propunere de regulament al Parlamentului European și al Consiliului de instituire a interoperabilității între sistemele de informații ale Uniunii Europene pentru securitate, frontiere și gestionarea migrației.

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

Afaceri interne (titlul 18)

1.3. Tipul propunerii/inițiativei

X Propunerea/inițiativa se referă la **o acțiune nouă**

☐ Propunerea/inițiativa se referă la **o acțiune nouă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare**[78]

☐ Propunerea/inițiativa se referă la **prelungirea unei acțiuni existente**

☐ Propunerea/inițiativa se referă la **o acțiune reorientată către o acțiune nouă**

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) strategic(e) multianual(e) al(e) Comisiei vizat(e) de propunere/inițiativă

Gestionarea frontierelor – salvarea de vieți omenești și securizarea frontierelor externe

Componentele necesare asigurării interoperabilității creează oportunitatea unei mai bune utilizări a informațiilor conținute în sistemele existente ale UE în materie de securitate, frontiere și gestionare a migrației. Cu ajutorul acestor măsuri se evită în special situațiile în care o persoană este înregistrată cu identități diferite în sisteme diferite. În prezent, identificarea unică a unei persoane este posibilă în cadrul unui anumit sistem, dar nu și între sisteme. Acest lucru poate duce la luarea unor decizii eronate de către autorități sau, invers, la ascunderea identității reale a unor călători de rea credință.

Îmbunătățirea schimbului de informații

Măsurile propuse prevăd, de asemenea, pentru serviciile de aplicare a legii, un acces la aceste date simplificat, dar supus în continuare anumitor limitări. Se propune un singur set de condiții, spre deosebire de situația actuală, când, pentru accesarea fiecărei colecții de date, trebuie respectat un alt set de condiții.

1.4.2. Obiectiv(e) specific(e) și obiectivul specific nr. [ ]

Prin crearea componentelor necesare interoperabilității se urmărește îndeplinirea următoarelor obiective generale:

(a) îmbunătățirea gestionării frontierelor externe,

(b) contribuția la prevenirea și combaterea migrației neregulamentare și

(c) contribuția la asigurarea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție al Uniunii, inclusiv menținerea siguranței publice și a ordinii publice și garantarea securității pe teritoriul statelor membre.

[78] Astfel cum sunt menționate la articolul 54 alineatul (2) litera (a) sau (b) din Regulamentul financiar.

Obiectivele legate de asigurarea interoperabilității sunt realizate prin:

(a) asigurarea identificării corecte a persoanelor;

(b) contribuirea la combaterea cazurilor de fraudă de identitate;

(c) îmbunătățirea și armonizarea cerințelor în materie de calitate a datelor din sistemele de informații ale UE;

(d) facilitarea implementării, din punct de vedere tehnic și operațional, de către statele membre a sistemelor de informații actuale și viitoare ale UE;

(e) consolidarea și simplificarea condițiilor privind securitatea și protecția datelor care guvernează respectivele sisteme de informații ale UE și sporirea uniformității acestor condiții;

(f) simplificarea și uniformizarea condițiilor de acces la EES, VIS, ETIAS și Eurodac în scopul asigurării respectării legii;

(g) sprijinirea realizării scopurilor pentru care au fost instituite EES, VIS, ETIAS, Eurodac, SIS și sistemul ECRIS-TCN.

Activitatea (activitățile) ABM/ABB în cauză

Capitolul „Securitate și protecția libertăților”: Securitate internă

1.4.3. Rezultatul (rezultatele) și impactul preconizate

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

Obiectivele generale ale acestei inițiative rezultă din cele două obiective înscrise în tratat:

1. îmbunătățirea gestionării frontierelor externe Schengen, pe baza Agendei europene privind migrația și a comunicărilor ulterioare, inclusiv a Comunicării privind menținerea și consolidarea spațiului Schengen.

2. participarea la securitatea internă a Uniunii Europene, pe baza Agendei europene privind securitatea și a activității Comisiei în vederea realizării unei uniuni a securității efective și autentice.

Obiectivele de politică specifice ale acestei inițiative privind interoperabilitatea

sunt:

1. să asigure accesul rapid, continuu, sistematic și controlat al utilizatorilor finali, în special al polițiștilor de frontieră, al agenților responsabili cu aplicarea legii, al funcționarilor din cadrul serviciilor de imigrație și al autorităților judiciare, la informațiile de care au nevoie pentru a-și îndeplini sarcinile;

2. să ofere o soluție pentru detectarea identităților multiple legate de același set de date biometrice, care să faciliteze identificarea corectă a persoanelor de bună credință și să combată cazurile de fraudă de identitate;

3. să faciliteze controalele de identitate efectuate asupra resortisanților țărilor terțe pe teritoriul unui stat membru, de către autoritățile polițienești și

4. să faciliteze și să simplifice accesul autorităților de aplicare a legii la sistemele de informații de la nivelul UE care nu intră în sfera asigurării respectării legii, atunci când acest lucru este necesar pentru prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor grave și infracțiunilor de terorism.

Pentru îndeplinirea obiectivului specific 1, se va dezvolta portalul european de căutare (ESP).

Pentru îndeplinirea obiectivului specific 2, se va institui detectorul de identități multiple (MID), care va beneficia de sprijinul registrului comun de date de identitate (CIR) și al serviciului comun de comparare a datelor biometrice (BMS comun).

Pentru îndeplinirea obiectivului specific 3, funcționarii autorizați vor avea acces la CIR în scopul identificării.

Pentru îndeplinirea obiectivului 4, CIR va conține o funcționalitate de marcare vizuală a rezultatelor pozitive („hit-flag”), care va permite o abordare în două etape a accesului autorităților de aplicare a legii la sistemele de gestionare a frontierelor.

Pe lângă aceste patru componente necesare asigurării interoperabilității, la îndeplinirea obiectivelor prezentate în secțiunea 1.4.2 vor contribui, de asemenea, instituirea și guvernanța formatului universal pentru mesaje (UMF) ca standard UE pentru dezvoltarea de sisteme de informații în domeniul justiției și afacerilor interne și instituirea unui registru central de raportare și statistici (CRRS).

1.4.4. Indicatori de rezultat și de impact

A se preciza indicatorii care permit monitorizarea punerii în aplicare a propunerii/inițiativei.

Fiecare dintre măsurile propuse necesită dezvoltarea, urmată de întreținerea și exploatarea componentei respective.

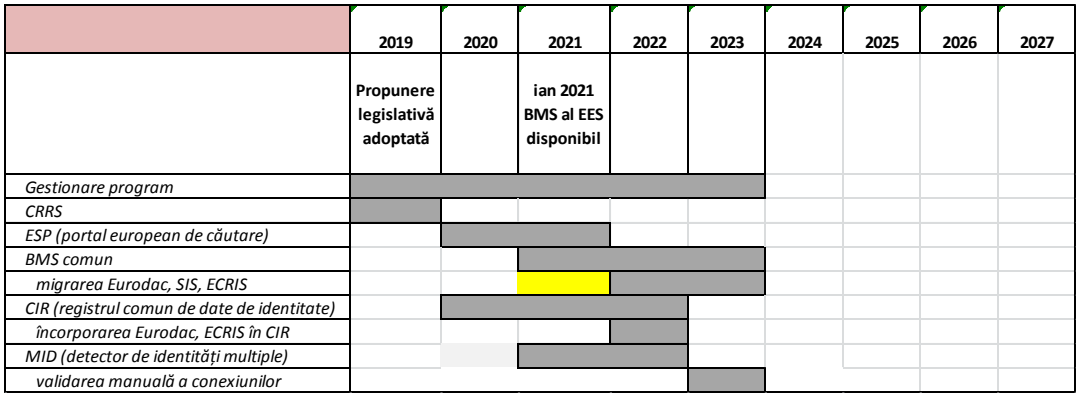
În faza de dezvoltare

Dezvoltarea fiecărei componente se va încheia odată ce vor fi îndeplinite condițiile de bază, și anume după ce propunerea legislativă va fi adoptată de colegiuitori și vor fi îndeplinite cerințele tehnice, deoarece unele componente nu pot fi instituite decât după ce o alta este disponibilă.

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

Până la sfârșitul anului 2017, propunerea se trimite colegiuitorilor în vederea adoptării. Prin analogie cu timpul necesar adoptării altor propuneri, se preconizează că procesul de adoptare va fi finalizat în cursul anului 2018.

În această ipoteză, demararea perioadei de dezvoltare este fixată la începutul anului 2019 (= T0); va exista astfel un punct de referință, nu date absolute, de la care se vor calcula perioadele. În cazul în care colegiuitorii adoptă proiectul la o dată ulterioară, întregul calendar se modifică în consecință. Pe de altă parte, BMS comun trebuie să fie disponibil înainte de finalizarea CIR și MID. Duratele de dezvoltare sunt indicate în tabelul de mai jos:



(Caseta în galben se referă la o sarcină specifică Eurodac.)

— registrul central de raportare și statistici (CRRS) – termen de finalizare: T0 + 12 luni (2019-2020)

— portalul european de căutare (ESP) – termen de finalizare: T0 + 36 de luni (2019-2021)

— serviciul comun de comparare a datelor biometrice (BMS comun) urmează să fie instituit pentru început pentru realizarea sistemului de intrare/ieșire (EES). Atunci când se va încheia această etapă, aplicațiile care vor utiliza BMS comun vor trebui actualizate, iar datele conținute în sistemul de identificare automată a amprentelor digitale (AFIS) al SIS, în AFIS Eurodac și în sistemul ECRIS-TCN vor trebui migrate în BMS comun. Termenul de finalizare este sfârșitul anului 2023.

— Registrul comun de date de identitate (CIR) este creat pentru început în cursul implementării EES. După finalizarea EES, datele din Eurodac și ECRIS vor fi încorporate în CIR. Termenul de finalizare este sfârșitul anului 2022 (disponibilitatea BMS comun + 12 luni).

— Detectorul de identități multiple (MID) va fi creat după ce CIR va fi operațional. Termenul de finalizare este sfârșitul anului 2022 (disponibilitatea BMS comun + 24 de luni), dar perioada de validare a conexiunilor dintre identitățile propuse de MID va necesita

mobilizarea foarte multor resurse. Fiecare dintre conexiunile estimate trebuie validată manual. Această operațiune se va încheia la sfârșitul anului 2023.

Perioada de funcționare efectivă începe odată ce se va finaliza perioada de dezvoltare indicată mai sus.

Exploatare

Indicatorii referitori la fiecare dintre obiectivele specifice menționate la punctul 1.4.3 sunt următoarele:

1. Obiectiv specific: accesul rapid, fără sincope și sistematic la sursele de date autorizate

— Numărul de cazuri de utilizare executate (= numărul de căutări care pot fi tratate de ESP) într-o anumită perioadă de timp.

— Numărul de căutări tratate de ESP în comparație cu numărul total de căutări (prin ESP și direct în sisteme) într-o anumită perioadă de timp.

2. Obiectiv specific: detectarea identităților multiple

— Numărul de identități care corespund unui același set de date biometrice în comparație cu numărul de identități cu informații biografice într-o anumită perioadă de timp.

— Numărul de cazuri de fraudă de identitate detectate în comparație cu numărul de identități conexate și numărul total de identități într-o anumită perioadă de timp.

3. Obiectiv specific: facilitarea identificării resortisanților țărilor terțe

— Numărul controalelor de identificare efectuate în comparație cu numărul total de tranzacții într-o anumită perioadă de timp.

4. Obiectiv specific: simplificarea accesului la sursele de date autorizate în scopul aplicării legii

— Numărul de accesări aferente „etapei 1” (= verificarea prezenței datelor) în scopul aplicării legii într-o anumită perioadă de timp.

— Numărul de accesări aferente „etapei 2” (= consultarea efectivă a datelor din sistemele UE din domeniu) în scopul aplicării legii într-o anumită perioadă de timp.

5. Obiectiv transversal suplimentar: îmbunătățirea calității datelor și utilizarea datelor pentru o mai bună elaborare a politicilor

— Publicarea periodică de rapoarte de monitorizare a calității datelor.

— Numărul solicitărilor *ad hoc* de informații statistice într-o anumită perioadă de timp.

1.5. Motivele propunerii/inițiativei

1.5.1. Cerință (cerințe) de îndeplinit pe termen scurt sau lung

Astfel cum s-a demonstrat în evaluarea impactului care însoțește prezenta propunere legislativă, respectivele componente propuse sunt necesare pentru realizarea interoperabilității:

• Pentru a se îndeplini obiectivul de a asigura accesul rapid, fără sincope, sistematic și controlat al utilizatorilor autorizați la sistemele de informații relevante, ar trebui să se creeze un portal european de căutare (ESP) care să aibă la bază BMS comun, portal care să permită efectuarea de căutări în toate bazele de date.

• Pentru a se îndeplini obiectivul de a facilita verificarea identității resortisanților țărilor terțe de către agenții autorizați pe teritoriul unui stat membru, ar trebui creat un registru comun de date de identitate (CIR), care să conțină setul minim de date de identificare și să aibă la bază același BMS comun.

• Pentru a se îndeplini obiectivul de a detecta identitățile multiple care corespund aceluiași set de date biometrice, cu scopul dublu de a facilita controalele de identitate pentru călătorii de bună credință și de a combate fraudele de identitate, ar trebui creat un detector de identități multiple (MID) care să conțină conexiunile între identitățile multiple din diferitele sisteme.

• Pentru a se îndeplini obiectivul de a facilita și simplifica accesul autorităților de aplicare a legii la sistemele de informații care nu intră în sfera asigurării respectării legii, în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor grave și a infracțiunilor de terorism, în registrul comun de date de identitate (CIR) ar trebui inclusă o funcționalitate de marcare vizuală a rezultatelor pozitive („hit-flagging”).

Întrucât trebuie îndeplinite toate obiectivele, soluția completă constă într-o combinație între ESP, RPA (cu marcarea vizuală a rezultatelor pozitive), toate acestea având la bază BMS comun.

1.5.2. Valoarea adăugată a intervenției Uniunii (aceasta poate rezulta din diferiți factori, precum câștigurile în materie de coordonare, securitatea juridică, o mai mare eficacitate sau existența unor complementarități). În sensul prezentului punct, „valoarea adăugată a intervenției Uniunii” reprezintă valoarea rezultată din intervenția Uniunii, care se adaugă valorii care ar fi fost altfel creată numai de statele membre.

Este necesar să se acționeze la nivel european, întrucât sistemele care fac obiectul propunerii privind interoperabilitatea sunt sisteme utilizate de mai multe state membre: fie de toate statele membre (Eurodac), fie de toate statele membre care fac parte din spațiul Schengen (EES, VIS, ETIAS și SIS). Prin definiție, pur și simplu nu se poate acționa la un alt nivel.

Principala valoare adăugată scontată constă în eliminarea cazurilor de fraudă de identitate, repertorierea cazurilor în care o persoană a utilizat identități diferite pentru a intra în UE și evitarea situațiilor în care persoane de bună credință sunt confundate cu persoane de rea credință cu același nume. O valoare adăugată suplimentară este că interoperabilitatea propusă aici permite o implementare și întreținere mai ușoară a sistemelor informatice la scară largă ale UE. În ceea ce privește serviciile de aplicare a legii, măsurile propuse ar trebui să aibă drept rezultat un acces mai frecvent și mai eficace la date specifice în cadrul sistemelor informatice la scară largă ale UE. La nivel operațional, calitatea datelor poate fi menținută și îmbunătățită doar dacă este monitorizată. De asemenea, în ceea ce privește procesul de elaborare a politicilor și de luare a deciziilor, trebuie create condițiile necesare pentru efectuarea de interogări *ad hoc* de date anonimizate.

O analiză costuri-beneficii face parte din evaluarea impactului și, ținându-se seama numai de beneficiile care pot fi cuantificate, beneficiile preconizate, care pot fi estimate la aproximativ 77,5 milioane EUR pe an, le revin în principal statelor membre. Aceste beneficii rezultă, în principal, din:

– reducerea costului modificărilor care ar urma să fie aduse aplicațiilor naționale atunci când sistemul central va fi operațional (estimată la 6 milioane EUR pe an pentru serviciile informatice ale statelor membre);

– reducerea costurilor datorită instituirii unui BMS central comun, în locul unui BMS pentru fiecare sistem central, care conține date biometrice (estimată la 1,5 milioane EUR pe an și economii punctuale de 8 milioane EUR pentru eu-LISA);

– economiile de cost legate de identificarea identităților multiple în comparație cu situația în care același rezultat ar fi obținut fără mijloacele propuse. Acest lucru ar genera economii de cel puțin 50 de milioane EUR pe an pentru administrațiile statelor membre în ceea ce privește gestionarea frontierelor, migrația și aplicarea legii;

– economii de costuri legate de formarea unui grup mare de utilizatori finali, în comparație cu situația unor nevoi recurente de formare, estimate la 20 de milioane EUR pe an pentru administrațiile statelor membre în ceea ce privește gestionarea frontierelor, migrația și aplicarea legii.

1.5.3. Învățăminte desprinse din experiențele anterioare similare

În urma dezvoltării Sistemului de informații Schengen de a doua generație (SIS II) și a Sistemului de informații privind vizele (VIS), am desprins următoarele învățăminte:

1. Ca o posibilă garanție împotriva depășirii costurilor și a întârzierilor care ar rezulta din modificarea cerințelor, niciun nou sistem de informații în spațiul de libertate, securitate și justiție, în special dacă implică un sistem informatic la scară largă, nu ar trebui dezvoltat înainte de adoptarea definitivă a instrumentelor juridice care stau la baza sistemului și care îi stabilesc scopul, domeniul de aplicare, funcțiile și detaliile tehnice.

2. Pentru SIS II și VIS, dezvoltarea națională în statele membre putea fi cofinanțată prin Fondul pentru frontierele externe (FFE), dar acest lucru nu a fost obligatoriu. Prin urmare, nu s-a putut avea o imagine de ansamblu asupra progreselor înregistrate în statele membre care nu au prevăzut activitățile respective în programarea lor multianuală sau a căror programare nu a fost suficient de precisă. De aceea, acum se propune rambursarea de către Comisie a tuturor costurilor de integrare suportate de statele membre, astfel încât aceasta să poată monitoriza progresul acestor dezvoltări.

3. Pentru a facilita coordonarea generală a implementării, pentru toate schimburile de mesaje propuse între sistemele naționale și sistemele centrale se vor reutiliza rețelele existente și interfața uniformă națională.

1.5.4. Compatibilitatea și posibila sinergie cu alte instrumente corespunzătoare

Compatibilitatea cu actualul CFM

Regulamentul de instituire în cadrul FSI a sprijinului pentru frontiere este instrumentul financiar în care a fost inclus bugetul alocat punerii în aplicare a inițiativei privind interoperabilitatea.

Articolul 5 litera (b) din acest regulament prevede faptul că 791 de milioane EUR urmează să fie utilizate prin intermediul unui program pentru dezvoltarea de sisteme informatice ce au la bază sisteme informatice existente și/sau noi de sprijin pentru gestionarea fluxurilor migratorii la frontierele externe, sub rezerva adoptării actelor legislative relevante ale Uniunii și în condițiile stabilite la articolul 15. Din 791 de milioane EUR, 480,2 milioane EUR sunt rezervate dezvoltării EES, 210 milioane EUR dezvoltării ETIAS și 67,9 milioane EUR revizuirii SIS II. Restul (32,9 milioane EUR) va fi realocat folosindu-se mecanismele ISF-B. Prezenta propunere solicită 32,1 milioane EUR pentru perioada rămasă din actualul cadru financiar multianual, sumă care se încadrează în bugetul restant.

Prezenta propunere necesită un buget total de 424,7 milioane EUR (inclusiv rubrica 5) pentru perioada 2019-2027. Actualul CFM acoperă doar anii 2019 și 2020. Costurile au

fost însă estimate inclusiv până în 2027, pentru a oferi o imagine avizată asupra consecințelor financiare ale acestei propuneri, fără a afecta următorul cadru financiar multianual.

Bugetul solicitat pentru o perioadă de nouă ani se ridică la 424,7 milioane EUR, fiind acoperite și următoarele posturi:

(1) 136,3 milioane EUR pentru statele membre, care acoperă modificările ce trebuie aduse sistemelor lor naționale în vederea utilizării componentelor necesare pentru asigurarea interoperabilității, interfața NUI furnizată de eu-LISA și un buget pentru formarea comunității substanțiale a utilizatorilor finali. Nu există niciun impact asupra CFM actual, întrucât finanțarea se va acorda începând din 2021.

(2) 4,8 milioane EUR pentru Agenția EBCG, ce va găzdui o echipă de specialiști care, în decurs de un an (2023), vor valida conexiunile dintre identități în momentul în care MID va fi operațional. Activitățile echipei pot fi asociate cu activitatea de dezambiguizare a identității, atribuită Agenției EBCG în propunerea privind ETIAS. Nu există niciun impact asupra CFM actual, întrucât finanțarea se va acorda începând din 2021.

(3) 48,9 milioane EUR pentru Europol, care acoperă costurile de modificare a sistemelor informatice ale Europol pentru a face față volumului de mesaje care urmează să fie manipulate și creșterii nivelurilor de performanță. Componentele necesare asigurării interoperabilității vor fi utilizate de ETIAS pentru a consulta datele Europol. Cu toate acestea, capacitatea de prelucrare a informațiilor de care dispune în prezent Europol nu este adaptată volumelor mari (în medie, 100 000 de interogări pe zi) și nici timpului de răspuns mai scurt. 9,1 milioane EUR sunt prevăzute în actualul CFM.

(4) 2,0 de milioane EUR pentru CEPOL, în vederea pregătirii cursurilor de formare și a formării personalului operațional. Se prevede suma de 0,1 milioane EUR în 2020.

(5) 225,0 de milioane EUR pentru eu-LISA, care acoperă costul total al dezvoltării programului ce constă în implementarea celor cinci componente necesare pentru asigurarea interoperabilității (68,3 milioane EUR), costurile de întreținere din momentul în care aceste componente vor fi lansate până în 2027 (56,1 milioane EUR), un buget specific de 25,0 de milioane EUR pentru migrarea datelor din sistemele existente către BMS comun și costurile suplimentare pe care le presupun actualizarea NUI, rețeaua, cursurile de formare și reuniunile. Un buget specific de 18,7 milioane EUR acoperă costurile aferente modernizării și exploatării ECRIS-TCN în condiții de disponibilitate ridicată începând din 2022. Din această sumă totală, 23,0 milioane EUR sunt prevăzute pentru actualul CFM.

(6) 7,7 milioane EUR pentru DG HOME, destinate să acopere o creștere limitată a personalului și costurile conexe în perioada de dezvoltare a diferitelor componente, întrucât Comisia va fi responsabilă și de comitetul care se ocupă de UMF (formatul universal pentru mesaje). Acest buget, care se înscrie în rubrica 5, nu va fi acoperit de bugetul FSI. Cu titlu informativ, 2,0 milioane EUR sunt datorate în perioada 2019-2020.

Compatibilitatea cu inițiativele anterioare

Această inițiativă este compatibilă cu următoarele:

În aprilie 2016, Comisia a prezentat o **comunicare intitulată *„Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”*** pentru a soluționa o serie de deficiențe structurale legate de sistemele de informații. Trei acțiuni s-au întreprins în urma acesteia:

În primul rând, Comisia **a luat măsuri pentru a consolida și pentru a maximiza beneficiile sistemelor de informații existente**. În decembrie 2016, Comisia a adoptat

propuneri menite să consolideze în continuare actualul Sistem de informații Schengen (SIS). Între timp, în urma propunerii Comisiei din mai 2016, s-au accelerat negocierile cu privire la revizuirea temeiului juridic pentru Eurodac – baza de date dactiloscopice a UE în materie de azil. O propunere pentru un nou temei juridic pentru Sistemul de informații privind vizele (VIS) este, de asemenea, în curs de elaborare și urmează să fie prezentată în cel de al doilea trimestru al anului 2018.

În al doilea rând, Comisia a propus **noi sisteme de informații pentru a se remedia lacunele identificate** în arhitectura UE de gestionare a datelor. Negocierile privind propunerea Comisiei din aprilie 2016 privind instituirea Sistemului de intrare/ieșire (EES)[79] – menită să îmbunătățească procedurile de verificare la frontiere – s-au încheiat încă din iulie 2017, când colegiuitorii au ajuns la un acord politic, confirmat de Parlamentul European în octombrie 2017 și adoptat de Consiliu în noiembrie 2017. În noiembrie 2016, Comisia a prezentat, de asemenea, o propunere privind instituirea Sistemului european de informații și de autorizare privind călătoriile (ETIAS)[80]. Prezenta propunere are scopul de a întări controalele de securitate efectuate în cazul călătorilor scutiți de viză prin faptul că permite efectuarea de verificări prealabile în vederea depistării cazurilor de migrație neregulamentară și de controale de securitate. În prezent, aceasta face obiectul negocierilor de către colegiuitori. În iunie 2017, s-a propus instituirea Sistemului european de informații cu privire la cazierele judiciare ale resortisanților țărilor terțe (sistemul ECRIS-TCN)[81], pentru a remedia deficiențele identificate în ceea ce privește schimbul de informații între statele membre privind resortisanții țărilor terțe condamnați.

În al treilea rând, Comisia a depus eforturi **în vederea realizării interoperabilității sistemelor de informații**, punând accentul pe cele patru opțiuni prezentate în comunicarea din aprilie 2016[82] pentru a realiza interoperabilitatea. Trei dintre cele patru opțiuni sunt ESP, CIR și BMS comun. Ulterior, a devenit evident că trebuie să se facă o distincție între CIR ca bază de date de identitate și o nouă componentă care identifică identitățile multiple ce corespund aceluiași identificator biometric (MID). Astfel, cele patru componente sunt în prezent: ESP, CIR, MID și BMS comun.

Sinergia

Sinergia este înțeleasă aici ca beneficiul realizat prin reutilizarea soluțiilor existente și prin evitarea de noi investiții.

Există o sinergie importantă între aceste inițiative și dezvoltarea EES și a ETIAS.

În ceea ce privește funcționarea EES, se creează un dosar individual pentru fiecare resortisant al unei țări terțe care intră în spațiul Schengen pentru o ședere de scurtă durată. În acest scop, actualul sistem de comparare a datelor biometrice utilizat pentru VIS, care conține modelele de amprente digitale pentru toți călătorii care trebuie să dețină viză, se va extinde, pentru a include datele biometrice ale călătorilor care sunt scutiți de obligația de a deține viză. BMS comun este astfel, din punct de vedere conceptual, o versiune și mai generalizată a comparatorului de date biometrice care va fi dezvoltat în cadrul EES. Modelele biometrice conținute în comparatorul de date biometrice al SIS și Eurodac vor fi apoi migrate (acesta este termenul tehnic atunci când datele sunt transferate dintr-un sistem în altul) în acest BMS comun. Conform datelor puse la dispoziție de furnizor, stocarea în baze de date separate costă în medie 1 EUR pe set de date biometrice (teoretic, există 200 de milioane de seturi de date în total), în timp ce costul mediu scade la 0,35 EUR pe set de

[79] COM (2016)194 din 6 aprilie 2016.
[80] COM (2016)731 din 16 noiembrie 2016.
[81] COM (2017)344 din 29 iunie 2017.
[82] COM (2016)205 din 6 aprilie 2016.

date biometrice atunci când se creează o soluție de tip BMS comun. Costurile mai ridicate ale componentelor hardware necesare pentru un volum mare de date vor contrabalansa în parte aceste avantaje, dar, în final, se estimează că, pentru BMS comun, costurile vor fi cu 30 % mai mici decât costurile aferente stocării aceloraşi date în mai multe sisteme BMS mai mici.

Pentru funcționarea ETIAS, una dintre componente trebuie să fie disponibilă pentru interogarea unui set de sisteme ale UE. Fie se utilizează ESP, fie se dezvoltă o componentă specifică în cadrul propunerii privind ESP. Propunerea privind interoperabilitatea permite construirea unei singure componente în loc de două.

De asemenea, există o sinergie obținută din reutilizarea aceleiaşi interfețe uniforme naționale (NUI) care este utilizată pentru EES şi ETIAS. NUI va trebui actualizată, dar va fi utilizată în continuare.

1.6. Durata și impactul financiar

☐ Propunere/inițiativă pe **durată determinată**

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

– ☐ Impact financiar din AAAA până în AAAA

☒ Propunere/inițiativă pe **durată nedeterminată**

– Perioada de dezvoltare din 2019 până în 2023 inclusiv, urmată de funcționarea la scară largă.

– Durata impactului financiar este, prin urmare, prevăzută pentru perioada 2019 - 2027.

1.7. Modul (modurile) de gestiune preconizat(e)[83]

☒ **Gestiune directă** asigurată de către Comisie

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

– ☐ de către agențiile executive;

☒ **Gestiune partajată** cu statele membre

☒ **Gestiune indirectă** cu delegarea sarcinilor de execuție bugetară:

– ☐ țărilor terțe sau organismelor pe care le-au desemnat acestea;

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

– ☐ BEI și Fondului european de investiții;

– ☒ organismelor menționate la articolele 208 și 209 din Regulamentul financiar;

– ☐ 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, identificate în actul de bază relevant.

– *Dacă se indică mai multe moduri de gestiune, a se furniza detalii suplimentare în secțiunea „Observații“.*

Observații

Blocuri	Faza de dezvoltare	Faza de funcționare	Tipul de gestiune	Actori
Dezvoltarea și întreținerea (componentelor de interoperabilitate pentru sistemele centrale, formare profesională privind sistemul)	X	X	Indirectă	eu-LISA Europol CEPOL

[83] Explicațiile privind modurile de gestiune, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Blocuri	Faza de dezvoltare	Faza de funcționare	Tipul de gestiune	Actori
Migrarea datelor (migrarea modelelor biometrice către BMS comun), costurile de rețea, actualizarea NUI, organizarea de reuniuni și formare	X	X	Indirectă	eu-LISA
Validarea conexiunilor în momentul instituirii MID	X	–	Indirectă	EBCG
Personalizarea NUI, integrarea sistemelor naționale și formarea utilizatorilor finali	X	X	Partajată (sau directă) (1)	COM + Statele membre

(1) În acest instrument nu sunt incluse sume pentru faza de exploatare.

Perioada de dezvoltare începe în 2019 și durează până la realizarea fiecărei componente, între 2019 și 2023 (a se vedea secțiunea 1.4.4).

1. Gestiune directă asigurată de către DGT HOME: În perioada de dezvoltare, în cazul în care 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 activitățile 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 faza de dezvoltare, statele membre vor trebui să își adapteze sistemele naționale pentru a avea acces mai degrabă la ESP decât la sistemele individuale (acest lucru este valabil pentru mesajele trimise de către statele membre) și pentru a modifica răspunsurile la interogările pe care le lansează (mesajele primite de către statele membre). Se vor actualiza interfețele NUI existente, implementate pentru EES și ETIAS.

3. Gestiune indirectă: Agenția eu-LISA se va ocupa de partea de dezvoltare a tuturor componentelor informatice ale proiectului, și anume de componentele necesare asigurării interoperabilității, de actualizarea interfeței uniforme naționale (NUI) din fiecare stat membru, de actualizarea infrastructurii de comunicații dintre sistemele centrale și interfețele uniforme naționale, de migrarea modelelor biometrice din sistemele de comparare a datelor biometrice ale SIS și Eurodac către BMS comun și de activitatea aferentă de curățare a datelor.

În perioada de funcționare, eu-LISA va desfășura toate activitățile tehnice legate de întreținerea componentelor.

În cadrul Agenției Europene pentru Poliția de Frontieră și Garda de Coastă (EBCG) își va desfășura activitatea o echipă specială care se va ocupa de validarea conexiunilor odată ce MID va fi pus în funcțiune. Aceasta este o sarcină limitată în timp.

Europol se va ocupa de dezvoltarea și întreținerea sistemelor sale pentru a asigura interoperabilitatea cu ESP și ETIAS.

CEPOL pregătește materiale de curs și oferă cursuri de formare serviciilor operaționale adoptând modelul de formare a formatorilor.

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

A se preciza frecvența și condițiile aferente acestor dispoziții.

Norme de monitorizare și raportare pentru dezvoltarea și întreținerea altor sisteme:

1. Agenția eu-LISA se asigură că există proceduri care să permită monitorizarea dezvoltării componentelor necesare asigurării interoperabilității din perspectiva obiectivelor legate de planificare și costuri și monitorizarea funcționării componentelor din perspectiva obiectivelor legate de rezultatele tehnice, eficacitatea costurilor, securitate și calitatea serviciilor.

2. În termen de șase luni de la intrarea în vigoare a prezentului regulament și, ulterior, la fiecare șase luni în cursul etapei de dezvoltare a componentelor, eu-LISA va trebui să prezinte Parlamentului European și Consiliului un raport cu privire la situația la zi privind dezvoltarea fiecărei componente. După încheierea fazei de dezvoltare, se transmite Parlamentului European și Consiliului un raport în care se explică în detaliu modul în care au fost îndeplinite obiectivele, în special obiectivele legate de planificare și costuri, și în care se justifică eventualele abateri.

3. În vederea întreținerii tehnice, eu-LISA are acces la informațiile necesare legate de operațiunile de prelucrare a datelor efectuate în componente.

4. După patru ani de la punerea în funcțiune a ultimei componente implementate și, ulterior, o dată la patru ani, eu-LISA prezintă Parlamentului European, Consiliului și Comisiei un raport privind funcționarea tehnică a componentelor.

5. După cinci ani de la punerea în funcțiune a ultimei componente implementate și, ulterior, o dată la patru ani, Comisia realizează o evaluare generală și formulează eventuale recomandări. Această evaluare generală include: rezultatele obținute de componente din perspectiva obiectivelor de interoperabilitate, mentenanță, performanță și implicațiile financiare, precum și impactul asupra drepturilor fundamentale.

Comisia transmite raportul de evaluare Parlamentului European și Consiliului.

6. Statele membre și Europol furnizează agenției eu-LISA și Comisiei informațiile necesare pentru întocmirea rapoartelor menționate la alineatele (4) și (5), conform indicatorilor cantitativi predefiniți de către Comisie și/sau de către eu-LISA. Aceste informații nu periclitează metodele de lucru și nici nu includ informații care dezvăluie sursele, identitățile membrilor personalului sau investigațiile desfășurate de autoritățile desemnate.

7. Agenția eu-LISA furnizează Comisiei informațiile necesare pentru realizarea evaluărilor generale menționate la alineatul (5).

8. Respectând dispozițiile din legislația națională referitoare la publicarea informațiilor sensibile, fiecare stat membru și Europol întocmesc rapoarte anuale cu privire la eficacitatea accesului la sistemele UE de asigurare a aplicării legii, care conțin informații și statistici privind:

– scopul exact al consultării, inclusiv tipul infracțiunii de terorism sau al infracțiunii grave;

– motivele rezonabile invocate pentru a justifica suspiciunea că suspectul, autorul sau victima fac obiectul prezentului regulament;

– numărul solicitărilor de acces la componente în scopul aplicării legii;

– numărul și tipul de cazuri finalizate cu identificări reușite;

– necesitatea și utilizarea prevederii privind situația excepțională de urgență, precum și cazurile în care urgența respectivă nu a fost acceptată în urma verificării ex-post efectuate de punctul central de acces.

Rapoartele anuale ale statelor membre și ale Europol se transmit Comisiei până la data de 30 iunie a anului următor.

2.2. Sistemul de gestiune și de control

2.2.1. Riscul (riscurile) identificat(e)

Riscurile sunt cele legate de dezvoltarea informatică a cinci componente de către un contractant extern gestionat de eu-LISA. Acestea sunt riscuri tipice aferente proiectelor:

1. riscul ca proiectul să nu fie finalizat la timp;

2. riscul ca proiectul să nu se încadreze în buget;

3. riscul ca proiectul să nu fie realizat pe deplin sub toate aspectele sale.

Primul risc este cel mai important, întrucât o depășire a termenului înseamnă o creștere a costurilor, având în vedere faptul că majoritatea costurilor sunt legate de durată: cheltuielile cu personalul, costurile de licență plătite pe an etc.

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 cazul perioadelor 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:

1. în special, riscul ca respectivul contractant să nu reușească să aloce resurse suficiente proiectului sau să proiecteze și să dezvolte un sistem care să nu corespundă celor mai noi cerințe în domeniu;

2. riscul ca tehnicile și metodele administrative de gestionare a proiectelor informatice la scară largă să nu fie pe deplin respectate, în încercarea de a reduce costurile de către contractant;

3. în sfârșit, riscul ca respectivul contractant să se confrunte cu dificultăți financiare din motive independente de acest proiect nu poate fi complet eliminat.

Aceste riscuri sunt atenuate prin atribuirea contractelor pe baza unor criterii de calitate solide, prin verificarea referințelor contractanților și prin menținerea unei relații puternice 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.

2.2.2. Informații privind sistemul de control intern instituit

Agenția eu-LISA este menită să fie un centru de excelență în domeniul dezvoltării și al gestionării sistemelor informatice la scară largă. Aceasta execută activitățile legate de dezvoltarea și exploatarea diferitelor componente necesare asigurării interoperabilității, inclusiv de întreținerea interfeței uniforme naționale din statele membre.

În timpul fazei de dezvoltare, toate activitățile de dezvoltare vor fi executate de eu-LISA. Aceasta va cuprinde partea de dezvoltare a tuturor elementelor proiectului. Costurile legate de integrarea sistemelor din statele membre în cursul dezvoltării vor fi gestionate de Comisie în cadrul gestiunii partajate sau prin granturi.

În faza de exploatare, eu-LISA va fi responsabilă cu gestionarea tehnică și financiară a componentelor utilizate la nivel central, în special cu atribuirea și gestionarea contractelor. Comisia va gestiona fondurile destinate statelor membre pentru cheltuielile aferente unităților naționale prin intermediul FSI/Frontiere (programele naționale).

Pentru a se evita întârzierile la nivel național, trebuie prevăzută o guvernanță eficientă între toate părțile interesate înainte de începerea fazei de dezvoltare. Comisia pleacă de la premisa că o arhitectură interoperabilă trebuie definită de la începutul proiectului, pentru a fi aplicată în proiectele EES și ETIAS, întrucât aceste proiecte realizează și utilizează BMS comun, registrul comun de date de identitate și portalul european de căutare. Un membru al echipei de management de proiect al proiectului de interoperabilitate ar trebui să facă parte din structura de guvernanță a proiectelor EES și ETIAS.

2.2.3. Estimarea costurilor și a beneficiilor controalelor și evaluarea nivelului prevăzut de risc de eroare

Nu există nicio estimare în acest sens, întrucât controlul și atenuarea riscurilor constituie o sarcină inerentă structurii de guvernanță a proiectului.

2.3. Măsuri de prevenire a fraudelor și a neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate.

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

1. Pentru a combate frauda, corupția și alte activități ilegale, se aplică Regulamentul (CE) nr. 1073/1999.

2. Agențiile aderă la Acordul interinstituțional privind investigațiile interne efectuate de Oficiul European de Luptă Antifraudă (OLAF) și stabilesc, fără întârziere, dispozițiile corespunzătoare aplicabile tuturor angajaților agențiilor.

3. Deciziile privind finanțarea și acordurile și instrumentele de punere în aplicare ce decurg din acestea prevăd în mod explicit că atât Curtea de Conturi, cât și OLAF pot efectua, dacă este necesar, verificări la fața locului ale beneficiarilor de finanțări acordate de agenții și ale agenților responsabili de atribuirea finanțărilor respective.

În conformitate cu această dispoziție, Consiliul de administrație al Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție a adoptat, la 28 iunie 2012, decizia privind termenele și condițiile pentru investigațiile interne referitoare la prevenirea fraudei, a corupției și a oricărei alte activități ilegale care dăunează intereselor Uniunii.

Se va aplica strategia DG HOME de prevenire și detectare a fraudei.

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

ÎN PREZENTA FIȘĂ FINANCIARĂ LEGISLATIVĂ SE MENȚIONEAZĂ ÎN SCOP INFORMATIV IMPACTUL ESTIMAT ASUPRA CHELTUIELILOR ȘI PERSONALULUI PENTRU ANUL 2021 ȘI PERIOADA ULTERIOARĂ, FĂRĂ CA ACEST LUCRU SĂ ADUCĂ ATINGERE CADRULUI FINANCIAR MULTIANUAL URMĂTOR

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 cheltuielilor	Contribuție			
	Număr[Rubrica ……...……]	Dif./ Nedif[84].	Țări AELS[85]	Țări candidate[86]	Țări terțe	în sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar
3	18.02.01.03 – Frontiere inteligente	Dif.	Nu	Nu	Da	Nu
3	18.02.03 – Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă (Frontex)	Dif.	Nu	Nu	Da	Nu
3	18.02.04 – EUROPOL	Dif.	Nu	Nu	Nu	Nu
3	18.02.05 – CEPOL	Nedif.	Nu	Nu	Nu	Nu
3	18.02.07 – Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA)	Dif.	Nu	Nu	Da	Nu

[84] Dif. = credite diferențiate/Nedif. = credite nediferențiate.
[85] AELS: Asociația Europeană a Liberului Schimb.
[86] Țările candidate și, după caz, țările potențial candidate din Balcanii de Vest.

3.2. Impactul estimat asupra cheltuielilor

[Această secțiune trebuie completată folosind **foaia de calcul cuprinzând datele din buget care au caracter administrativ** (al doilea document din anexa la prezenta fișă financiară), care trebuie încărcată în DECIDE pentru consultarea interservicii.]

3.2.1. Sinteza impactului estimat asupra cheltuielilor

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual	3	Securitate și cetățenie

DG Migrație și Afaceri Interne (DG HOME)			Anul **2019**	Anul **2020**	Anul **2021**	Anul **2022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**Anul 2028**	**TOTAL**
• Credite operaționale													
18.02.01.03 – Frontiere inteligente	Angajamente	(1)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Plăți	(2)	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300
Credite cu caracter administrativ finanțate din bugetul unor programe specifice[87]													
Numărul liniei bugetare		(3)											
TOTAL credite pentru DG Migrație și Afaceri Interne	Angajamente	=1+1a +3)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Plăți	=2+2a +3	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300

Cheltuielile vor acoperi costurile aferente:

– adaptării interfețelor uniforme naționale (NUI) a căror dezvoltare este finanțată în temeiul propunerii privind EES, unei sume bugetate pentru schimbările aduse sistemelor statelor membre generate de modificările sistemelor centrale și unei sume bugetate pentru formarea utilizatorilor finali.

[87] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

18.0203 – EBCG			Anul2 **019**	Anul **2020**	Anul2 **021**	Anul2 **022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**TOTAL**
Titlul 1: Cheltuieli cu personalul	Angajamente	(1)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
	Plăți	(2)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
Titlul 2: Cheltuieli de infrastructură și de funcționare	Angajamente	(1a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
	Plăți	(2a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
Titlul 3: Cheltuieli operaționale	Angajamente	(3a)	0	0	0	0,183	2,200	0	0	0	0	2,383
	Plăți	(3b)	0	0	0	0,183	2,200	0	0	0	0	2,383
TOTAL credite pentru Europol	(Total angajamente = Total plăți)	=1+1a+3a	**0**	**0**	**0**	**0,776**	**4,744**	**0,402**	**0**	**0**	**0**	**5,923**

– Bugetul pentru EBCG acoperă cheltuielile aferente unei echipe care va avea responsabilitatea să valideze conexiunile generate de MID (detectorul de identități multiple) din datele existente (aproximativ 14 milioane de înregistrări). Numărul conexiunilor care trebuie validate manual este estimat la 550 000. Echipa care va avea responsabilități în acest sens se va adăuga echipei EBCG instituite pentru ETIAS întrucât, din punct de vedere funcțional, cele două echipe sunt apropiate și astfel se evită costurile legate de crearea unei echipe noi. Se preconizează că activitatea va începe în 2023, prin urmare, se vor recruta agenți contractuali cu până la 3 luni în avans, pe o perioadă care se încheie până la 2 luni după terminarea activității legate de migrare. S-a considerat că o altă parte a resurselor umane necesare va fi recrutată cu statut de consultant și nu de agent contractual, ceea ce explică costul menționat la titlul 3 pentru 2023. S-a considerat că persoanele cu statut de consultant vor fi angajate cu o lună înainte de începerea activității. Detalii suplimentare privind efectivele de personal vor fi furnizate ulterior.

– Prin urmare, titlul 1 include costurile aferente unui număr de 20 de angajați interni și dispoziții pentru suplimentarea personalului de management și suport.

– Titlul 2 include costurile suplimentare aferente găzduirii celor 10 noi persoane angajate de contractant.

– Titlul 3 include onorariile aferente celor 10 persoane suplimentare angajate de contractant. Nu există alte tipuri de costuri incluse.

18.0204 – Europol			Anul2 **019**	Anul **2020**	Anul2 **021**	Anul2 **022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**TOTAL**

Titlul 1: Cheltuieli cu personalul	Angajamente	(1)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
	Plăți	(2)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
Titlul 2: Cheltuieli de infrastructură și de funcționare	Angajamente	(1a)	0	0	0	0	0	0	0	0	0	0
	Plăți	(2a)	0	0	0	0	0	0	0	0	0	0
Titlul 3: Cheltuieli operaționale	Angajamente	(3a)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
	Plăți	(3b)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
TOTAL credite pentru Europol	(Total angajamente = Total plăți)	=1+1a+3a	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860

Cheltuielile suportate de Europol vor asigura modernizarea capacităților sistemelor TIC de care dispune agenția astfel încât să poată face față volumului de mesaje care urmează a fi prelucrate, precum și creșterii necesare a nivelurilor de performanță (timpul de răspuns).

Titlul 1 - Cheltuielile cu personalul acoperă costurile aferente personalului suplimentar din domeniul TIC care urmează să fie recrutat pentru a consolida sistemele de informații ale Europol din motivele descrise anterior. Detalii suplimentare referitoare la repartizarea posturilor între agenți temporari și agenți contractuali, precum și competențele acestora sunt prezentate mai jos.

Titlul 3 include costurile aferente echipamentelor și programelor informatice necesare pentru a consolida sistemele de informații ale Europol. În prezent, sistemele informatice ale Europol deservesc o comunitate desemnată limitată, alcătuită din Europol, ofițerii de legătură ai Europol și investigatorii din statele membre, care utilizează aceste sisteme pentru analize și investigații. Prin implementarea interfeței QUEST (care va permite ESP să efectueze interogări în datele Europol) la un nivel de protecție de bază (în prezent, sistemele de informații ale Europol sunt acreditate până la nivelele „EU restricted” și „EU confidential”), sistemele de informații ale Europol vor fi puse la dispoziția unei comunități mult mai mari de utilizatori cu responsabilități în materie de asigurare a respectării legii. Pe lângă aceste majorări, ESP va fi utilizat de ETIAS pentru a efectua interogări automate în datele Europol pentru a prelucra autorizațiile de călătorie. Acest lucru va spori volumul interogărilor efectuate în datele Europol de la aproximativ 107 000 de interogări pe lună, câte sunt în prezent, la peste 100 000 de interogări pe zi, și va necesita, de asemenea, disponibilitatea 24 de ore din 24, șapte zile din șapte a sistemelor de informații ale Europol și timpi foarte scurți de răspuns pentru a îndeplini cerințele impuse de Regulamentul privind ETIAS. Majoritatea costurilor sunt limitate la perioada care precede intrarea în funcțiune a componentelor de interoperabilitate, însă unele angajamente în curs sunt necesare pentru a se asigura un nivel ridicat și continuu de disponibilitate a sistemelor de informații ale Europol. De asemenea, sunt necesare unele acțiuni de dezvoltare pentru implementarea componentelor de interoperabilitate de către Europol ca utilizator.

18.0205 – CEPOL			Anul2019	Anul 2020	Anul2021	Anul2022	Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	TOTAL
Titlul 1: Cheltuieli cu personalul	Angajamente	(1)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
	Plăți	(2)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Titlul 2: Cheltuieli de infrastructură și de funcționare	Angajamente	(1a)	0	0	0	0	0	0	0	0	0	0
	Plăți	(2a)	0	0	0	0	0	0	0	0	0	0
Titlul 3: Cheltuieli operaționale	Angajamente	(3a)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
	Plăți	(3b)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
TOTAL credite pentru CEPOL	(Total angajamente = Total plăți)	=1+1a+3a	0	0,144	0,384	0,482	0,208	0,208	0,208	0,208	0,208	2,050

Cursurile de formare coordonate centralizat la nivelul UE îmbunătățesc modul în care se derulează cursurile de formare la nivel național, aducând un plus de coerență, și, în consecință, asigură implementarea și utilizarea cu succes și corectă a componentelor de interoperabilitate. CEPOL, ca agenție a UE pentru formare în materie de aplicare a legii, este organismul potrivit pentru a oferi cursuri de formare la nivel central, european. Aceste cheltuieli acoperă pregătirea „formării formatorilor din statele membre", care vor trebui să utilizeze sistemele centrale atunci când acestea vor deveni interoperabile. Costurile includ sumele aferente unei creșteri reduse de personal din CEPOL, care va asigura coordonarea, gestionarea, organizarea și actualizarea cursurilor, precum și sumele aferente unei serii de sesiuni de formare pe an și pregătirii cursurilor online. Detalii cu privire la aceste costuri sunt prezentate mai jos. Efortul de formare este concentrat pe perioada care precede imediat punerea în funcțiune a sistemelor. Un efort continuu rămâne necesar după punerea în funcțiune a sistemelor, întrucât componentele de interoperabilitate trebuie întreținute și formatorii se schimbă, după cum a dovedit-o experiența dobândită cu ocazia cursurilor de formare organizate privind Sistemul de informații Schengen.

18.0207 – eu-LISA			Anul2019	Anul2020	Anul2021	Anul2022	Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	TOTAL
Titlul 1: Cheltuieli cu personalul	Angajamente	(1)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
	Plăți	(2)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
Titlul 2: Cheltuieli de	Angajamente	(1a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389

infrastructură și de funcționare	Plăți	(2a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Titlul 3: Cheltuieli operaționale	Angajamente	(3a)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
	Plăți	(3b)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
TOTAL credite pentru eu-LISA	(Total angajamente = Total plăți)	=1+1a+3a	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**

Aceste cheltuieli vor acoperi:

– Dezvoltarea și întreținerea celor patru componente de interoperabilitate incluse în propunerea legislativă [portalul european de căutare (ESP), serviciul comun de comparare a datelor biometrice (BMS), registrul comun de date de identitate (CIR) și detectorul de identități multiple (MID)], precum și a registrului central de raportare și statistici (CRRS). Agenția eu-LISA va acționa în calitate de reprezentant al proprietarului proiectului și își va pune la dispoziție personalul pentru elaborarea specificațiilor, selectarea contractanților, direcționarea activității acestora, transmiterea rezultatelor obținute în urma efectuării unei serii de teste și validarea acțiunilor efectuate.

– Costurile pe care le presupune migrarea datelor din sistemele existente către noile componente. Agenția eu-LISA nu are însă un rol direct în încărcarea inițială de date în MID (validarea conexiunilor), deoarece aceasta este o acțiune legată de conținutul de date în sine. Migrarea datelor biometrice din sistemele existente se referă la formatul și clasificarea datelor, nu la conținutul acestora.

– Costurile pentru modernizarea și exploatarea ECRIS-TCN la standardul de sistem cu o disponibilitate ridicată începând cu 2022. ECRIS-TCN este un sistem central care conține cazierele judiciare ale resortisanților țărilor terțe. Se preconizează că sistemul va fi disponibil până în 2020. Întrucât se preconizează ca ECRIS-TCN să poată fi accesat și de către componentele de interoperabilitate, acesta ar trebui să devină, la rândul său, un sistem cu o disponibilitate ridicată. Cheltuielile operaționale includ costurile suplimentare aferente îndeplinirii standardului de disponibilitate ridicată. În 2021 costurile aferente dezvoltării sistemului vor fi ridicate, ulterior fiind prevăzute costuri de întreținere și de exploatare cu caracter recurent. Aceste costuri nu sunt incluse în fișa financiară legislativă a documentului prin care se revizuiește Regulamentul de înființare a agenției eu-LISA[88], care include numai bugetele din perioada 2018-2020 și, prin urmare, nu se suprapune cu prezenta cerere bugetară.

[88] COM 2017/0145 (COD) Propunere de Regulament al Parlamentului European și al Consiliului privind Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție și de modificare a Regulamentului (CE) 1987/2006 și a Deciziei 2007/533/JAI a Consiliului, precum și de abrogare a Regulamentului (UE) 1077/2011

– Modelul cheltuielilor este rezultatul secvențierii proiectului. Întrucât diferitele componente nu sunt independente, dezvoltarea acoperă perioada 2019-2023. Cu toate acestea, din 2020 încep deja întreținerea și funcționarea primelor componente disponibile. Astfel se explică nivelul inițial scăzut al cheltuielilor, care crește ulterior și apoi se diminuează până la o valoare constantă.

– Cheltuielile din cadrul titlului 1 (cheltuieli cu personalul) respectă secvențierea proiectului: este nevoie de personal mai numeros pentru a realiza proiectul împreună cu contractantul (ale cărui cheltuieli sunt grupate la titlul 3). Atunci când proiectul este realizat, unei părți din echipa care a lucrat la realizarea acestuia i se vor încredința sarcini de evoluție și întreținere a sistemelor. În același timp, va spori personalul care se ocupă de exploatare a sistemelor nou livrate.

– Cheltuielile din cadrul titlului 2 (cheltuieli de infrastructură și de funcționare) includ spațiul suplimentar de birouri pentru găzduirea temporară a echipelor contractantului responsabile de dezvoltare, întreținere și exploatare. Variația în timp a cheltuielilor reflectă, prin urmare, și evoluția efectivelor de personal. Costurile aferente găzduirii de echipamente suplimentare au fost deja incluse în bugetul eu-LISA. De asemenea, nu există costuri suplimentare pentru găzduirea personalului eu-LISA, deoarece acestea sunt incluse în costurile standard de personal.

– Cheltuielile de la titlul 3 (cheltuieli operaționale) includ costurile suportate de contractant pentru dezvoltarea și întreținerea sistemului și achiziționarea de echipamente și programe informatice specifice.
  Costurile contractantului acoperă inițial studiile pentru specificarea componentelor, iar dezvoltarea începe cu o singură componentă (CRRS). În perioada 2020-2022, costurile cresc pe măsură ce tot mai multe componente sunt dezvoltate în paralel. Costurile nu se diminuează după vârful atins deoarece sarcinile legate de migrarea datelor sunt deosebit de dificile în portofoliul acestui proiect. Costurile contractantului se diminuează pe măsură ce sunt livrate componentele și acestea intră în faza de funcționare, care necesită o combinație stabilă de resurse.
  Simultan cu cheltuielile din cadrul titlului 3, nivelul cheltuielilor va spori mult în 2020 în comparație cu anul precedent, din cauza investiției inițiale în echipamentele și programele informatice necesare în cursul dezvoltării. Cheltuielile din cadrul titlului 3 (cheltuieli operaționale) cresc în 2021 și 2022 deoarece costurile de investiții în echipamente și programe informatice pentru mediile IT operaționale (producție și preproducție atât pentru unitatea centrală, cât și pentru unitatea centrală de rezervă) sunt suportate în anul anterior punerii în funcțiune efective a componentelor de interoperabilitate (CIR și, respectiv, MID) care presupun cerințe ridicate în materie de echipamente și programe informatice. Odată ce aceste sisteme devin operaționale, costurile aferente echipamentelor și programelor informatice vor fi, în principal, costuri de întreținere.

– Mai multe detalii sunt prezentate în continuare.

Rubrica din cadrul financiar multianual	**5**	„Cheltuieli administrative”

milioane EUR (cu trei zecimale)

		Anul **2019**	Anul **2020**	Anul **2021**	Anul **2022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**TOTAL**
DG HOME											
• Resurse umane Numărul liniei bugetare 18.01		0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Alte costuri administrative (reuniuni etc.)		0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
TOTAL pentru DG HOME	Credite	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

TOTAL credite **în cadrul RUBRICII 5** din cadrul financiar multianual	(Total angajamente = Total plăți)	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

milioane EUR (cu trei zecimale)

		Anul **2019**	Anul **2020**	Anul **2021**	Anul **2022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	Anul 2028	**TOTAL**
TOTAL credite în cadrul RUBRICILOR 1-5 din cadrul financiar multianual	Angajamente	**7,533**	**26,569**	**104,672**	**98,591**	**83,363**	**25,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**
	Plăți	**7,533**	**26,569**	**96,042**	**97,591**	**83,993**	**34,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**

3.2.2. Impactul estimat asupra creditelor operaționale

3.2.2.1. Impactul estimat asupra creditelor agenției EBCB

– ☐ 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 **2019**		Anul **2020**		Anul **2021**		Anul **2022**		Anul **2023**		Anul **2024**		Anul **2025**		Anul **2026**		Anul **2027**		**TOTAL**	
Agenția EBCG ⇩	Tip[89]	Costuri medii	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 1[90] Validarea de conexiuni																						
Numărul de persoane recrutate în calitate de experți pentru a valida conexiuni	Costurile aferente contractantului		0	0	0	0	0	0	0,8	0,183	10	2,200	0	0	0	0	0	0	0	0		2,383
Subtotal pentru obiectivul specific nr. 1			**0**	**0**	**0**	**0**	**0**	**0**	**0,8**	**0,183**	**10**	**2,200**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**2,383**

[89] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de stradă construiți etc.).

[90] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

Aceste cheltuieli vor acoperi:

- Recrutarea unui număr suficient de personal suplimentar (estimat la 10 experți) față de personalul intern (estimat la 20 de persoane) în vederea validării conexiunilor, care va fi găzduit de EBCG. Este prevăzută o singură lună pentru recrutare înainte de data de începere la care se prevede să se atingă nivelurile de personal necesare.

- Nu există alte costurile estimate aferente contractantului. Cheltuielile aferente programelor informatice necesare sunt incluse în costurile de achiziție a licenței pentru BMS comun. Nu există o capacitate specifică de prelucrare a echipamentelor informatice. Se presupune că personalul contractantului va fi găzduit de EBCG. De aceea, în cadrul titlului 2 s-a adăugat costul anual aferent unei suprafețe medii de 12 metri pătrați de persoană.

3.2.2.2. 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 **Europol** ⇩			Anul **2019**		Anul **2020**		Anul **2021**		Anul **2022**		Anul **2023**		Anul **2024**		Anul **2025**		Anul **2026**		Anul **2027**		**TOTAL**	
	Tip[91]	Costuri medii	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 1[92] Dezvoltarea și întreținerea sistemelor (Europol)																						
Mediul IT	Infrastructura					1,840		1,840		0,736		0,736		0,736		0,736		0,736		0,736		8,096
Mediul IT	Echipamente informatice					3,510		3,510		1,404		1,404		1,404		5,754		5,754		1,404		26,144
Mediul IT	Programe informatice					0,670		0,670		0,268		0,268		0,268		0,268		0,268		0,268		2,948

[91] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de stradă construiți etc.).

[92] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

Lucrări de dezvoltare	Contractant				0,360		0,360												0,720
Subtotal			**0**		**6,380**		**6,380**		**2,408**		**2,408**		**2,408**		**7,758**		**7,758**		**2,408**		**37,908**

Aceste cheltuieli vor acoperi necesitatea de a consolida sistemele de informații și infrastructura Europol pentru a face față numărului mai mare de interogări efectuate. Aceste costuri includ:

- îmbunătățirea securității și a infrastructurii rețelelor, a echipamentelor informatice (servere, stocare) și a programelor informatice (licențe). Aceste îmbunătățiri trebuie finalizate înainte ca portalul european de căutare și ETIAS să devină operaționale în 2021, costurile fiind repartizate în mod egal între 2020 și 2021. Începând cu 2022, ca bază de calcul pentru costurile de întreținere s-a folosit o rată anuală de întreținere de 20 %. În plus, s-a ținut cont de ciclul standard de cinci ani de înlocuire a echipamentelor informatice și a infrastructurii învechite;
- costurile contractantului aferente lucrărilor de dezvoltare pentru implementarea interfeței QUEST la un nivel de protecție de bază.

3.2.2.3. Impactul estimat asupra creditelor CEPOL

– ☐ 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 **CEPOL** ⇩			Anul **2019**		Anul **2020**		Anul **2021**		Anul **2022**		Anul **2023**		Anul **2024**		Anul **2025**		Anul **2026**		Anul **2027**		**TOTAL**	
	Tip[93]	Costuri medii	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 1[94] Elaborarea și oferirea de cursuri de formare																						
Numărul de cursuri de formare desfășurate în centre de formare externe	0,34 pe curs		0		1	0,040	4	0,136	8	0,272	2	0,068	2	0,068	2	0,068	2	0,068	2	0,068		0,788
Cursuri de formare online	0,02			0				0,040		0,002		0,002		0,002		0,002		0,002		0,002		0,052
Subtotal				**0**		**0,040**		**0,176**		**0,274**		**0,070**		**0,070**		**0,070**		**0,070**		**0,070**		**0,840**

[93] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de stradă construiți etc.).

[94] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

Pentru a se asigura implementarea uniformă și utilizarea soluțiilor de interoperabilitate, se vor organiza cursuri de formare atât la nivel central, european, de către CEPOL, cât și la nivel național, de către statele membre. Cheltuielile aferente cursurilor de formare organizate la nivelul UE includ:

- dezvoltarea unui program de formare comun care să fie utilizat de statele membre pentru cursurile de formare oferite la nivel național;

- activități de formare desfășurate în centre de formare externe, dedicate formatorilor. Într-o perioadă de doi ani după ce soluțiile de interoperabilitate vor deveni operaționale, se preconizează ca formarea să se deruleze pe o scară mai largă și ulterior să se organizeze anual două activități de formare în centre de formare externe;

- cursuri online care vor veni în completarea activităților de formare desfășurate în centre de formare externe la nivelul UE și al statelor membre.

3.2.2.4. 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 **eu-LISA** ⇩			Anul **2019**		Anul **2020**		Anul **2021**		Anul **2022**		Anul **2023**		Anul **2024**		Anul **2025**		Anul **2026**		Anul **2027**		**TOTAL**	
	Tip[95]	Costuri medii	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 1[96] Dezvoltarea componentelor de interoperabilitate																						
Sisteme dezvoltate	Contractant			1,800		4,930		8,324		4,340		1,073		1,000		0,100		0,020		0,020		21,607
Produse legate de programele informatice	Programe informatice			0,320		3,868		15,029		8,857		3,068		0,265		0,265		0,265		0,265		32,202
Produse legate de echipamentele informatice	Echipamente informatice			0,250		2,324		5,496		2,904		2,660		0,500		0		0		0		14,133
Formare în domeniul IT	Formare și altele			0,020		0,030		0,030		0,030		0,030		0,050		0,050		0,050		0,050		0,340

[95] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de stradă construiți etc.).

[96] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

Subtotal pentru obiectivul specific nr. 1		**2,390**		**11,151**		**28,879**		**16,131**		**6,830**		**1,815**		**0,415**		**0,335**		**0,335**		**68,281**

– Acest obiectiv include doar costurile pentru livrarea celor patru componente de interoperabilitate și a CRRS.

– Costurile pentru BMS comun au fost estimate luându-se în considerare ipoteza că EES care urmează a fi dezvoltat va servi drept sistem de bază pentru dezvoltare. Prin urmare, se intenționează reutilizarea licențelor aferente programelor informatice de biometrie (36 de milioane EUR) achiziționate pentru EES.

– În acest buget, BMS comun este considerat, din perspectivă bugetară, o prelungire a BMS pentru EES. Prin urmare, actuala fișă financiară include costul marginal al licențelor aferente programelor informatice (6,8 milioane EUR) care vor fi utilizate pentru a transfera cele aproximativ 20 de milioane de seturi de date biometrice din SIS AFIS (AFIS este sistemul de identificare automată a amprentelor digitale, adică corespondentul „BMS” din SIS), din Eurodac și din viitorul sistem ECRIS-TCN (Sistemul european de informații cu privire la cazierele judiciare pentru resortisanții țărilor terțe) în BMS livrat pentru EES. Costurile pentru integrarea diferitelor sisteme (SIS, Eurodac, ECRIS-TCN) în BMS comun sunt incluse în prezenta fișă financiară.

– Ca parte a lucrărilor ce vor fi desfășurate în perioada 2019-2020, agenției eu-LISA i se va solicita să găsească soluția tehnică exactă, care nu poate fi definită la momentul depunerii prezentei propuneri legislative, și să estimeze consecințele din punctul de vedere al costurilor pe care le-ar implica aplicarea soluției tehnice preferate. Acest lucru poate implica o modificare a estimării costurilor, astfel cum este furnizată în prezenta fișă.

– Toate componentele vor fi livrate până la sfârșitul anului 2023, acesta fiind motivul pentru care cheltuielile contractantului se reduc ajungând aproape la zero în acel moment. Rămâne numai o valoare reziduală pentru actualizarea recurentă a CRSS.

– În perioada 2019-2021, cheltuielile aferente programelor informatice cresc substanțial, întrucât trebuie acoperite costurile licențelor pentru diferitele medii necesare pentru preproducție, producție și testare, atât în unitatea centrală, cât și în unitatea de rezervă. În plus, prețul unor componente specifice și indispensabile ale programelor informatice este evaluat în funcție de numărul de „obiecte la care se face trimitere” (adică volumul de date). Întrucât baza de date va conține în final aproximativ 220 de milioane de identități, prețul programului informatic este proporțional cu acest volum de date.

A se indica obiectivele și realizările eu-LISA ⇩			Anul **2019**		Anul **2020**		Anul **2021**		Anul **2022**		Anul **2023**		Anul **2024**		Anul **2025**		Anul **2026**		Anul **2027**		**TOTAL**	
	Tip[97]	Costuri medii	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 2 Întreținerea și exploatarea componentelor de interoperabilitate																						
Menținerea sistemelor în stare	Contractant			0		0		0		1,430		2,919		2,788		2,788		2,788		2,788		15,501
Produse legate de programele informatice	Programe informatice			0		0,265		0,265		1,541		5,344		5,904		5,904		5,904		5,904		31,032
Produse legate de echipamentele informatice	Echipamente informatice			0		0,060		0,060		0,596		1,741		1,741		1,741		1,741		1,741		9,423
Formare în	Formare			0		0		0		0		0,030		0,030		0,030		0,030		0,030		0,150
Subtotal pentru obiectivul specific nr. 2				**0**		**0,325**		**0,325**		**3,567**		**10,034**		**10,464**		**10,464**		**10,464**		**10,464**		**56,105**

– Întreținerea începe de îndată ce se livrează o parte din componente. Prin urmare, bugetul aferent unui contractant care va asigura întreținerea este inclus din momentul în care este livrat ESP (în 2021). Bugetul aferent întreținerii crește pe măsură ce se livrează următoarele componente și apoi ajunge la un nivel mai mult sau mai puțin constant, reprezentând un procent (între 15 și 22 %) din investiția inițială.

[97] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de stradă construiți etc.).

– Întreținerea echipamentelor și programelor informatice începe din anul punerii în funcțiune a sistemelor: evoluția costurilor urmează o curbă similară celei pentru costurile contractanților.

A se indica obiectivele și realizările eu-LISA ⇩			Anul 2019		Anul 2020		Anul 2021		Anul 2022		Anul 2023		Anul 2024		Anul 2025		Anul 2026		Anul 2027		TOTAL	
	Tip[98]	Costuri medii	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 3[99] Migrarea datelor																						
Datele existente migrate din BMS	în BMS comun			0		0		0		7,000		3,000		0		0		0		0		10,000
Facilitarea migrării datelor existente în EDAC	Reconceperea și redezvoltarea EDAC			0		0		7,500		7,500				0		0		0		0		15,000
Subtotal pentru obiectivul specific nr. 3				**0**		**0**		**7,500**		**14,500**		**3,000**										**25,000**

– În cazul proiectului BMS comun, datele trebuie să fie migrate din alte motoare biometrice în BMS comun, întrucât acest sistem comun este mai eficace din punct de vedere operațional și, de asemenea, oferă un avantaj financiar în comparație cu ipoteza în care s-ar menține mai multe sisteme BMS de dimensiuni mai mici.

– Actuala logică de funcționare a Eurodac nu este clar separată de mecanismul de comparare a datelor biometrice, după cum este cazul sistemului BMS care operează cu VIS. Funcționarea internă a Eurodac și mecanismul prin care serviciile operaționale accesează serviciile de găsire a

[98] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de stradă construiți etc.).
[99] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

conexiunilor biometrice subiacente reprezintă o cutie neagră pentru publicul exterior și se bazează pe tehnologii brevetate. Nu va fi posibil să se migreze pur și simplu datele în BMS comun și să se păstreze nivelul operațional existent. Prin urmare, migrarea datelor presupune costuri semnificative pentru schimbarea mecanismelor prin care se efectuează schimburile cu aplicația centrală a Eurodac.

A se indica obiectivele și realizările **eu-LISA** ⇩			Anul **2019**		Anul **2020**		Anul **2021**		Anul **2022**		Anul **2023**		Anul **2024**		Anul **2025**		Anul **2026**		Anul **2027**		**TOTAL**	
	Tip[100]	Costuri medii	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 4[101] Rețea																						
Conexiuni de rețea	Configurarea rețelei			0		0		0		0,505										0		0,505
Traficul de rețea gestionat	Operațiuni în rețea			0		0						0,246		0,246		0,246		0,246		0,246		1,230
Subtotal pentru obiectivul specific nr. 4				**0**		**0**		**0**		**0,505**		**0,246**		**0,246**		**0,246**		**0,246**		**0,246**		**1,735**

– Componentele de interoperabilitate au doar un efect marginal asupra traficului în rețea. Din perspectiva datelor, se creează numai conexiuni între datele existente, ceea ce reprezintă un volum redus. Costul inclus aici reprezintă doar creșterea marginală a bugetului necesară, în plus față de bugetele aferente EES și ETIAS, pentru configurarea rețelei și pentru trafic.

[100] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de stradă construiți etc.).
[101] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

A se indica obiectivele și realizările eu-LISA ⇩			Anul **2019**		Anul **2020**		Anul **2021**		Anul **2022**		Anul **2023**		Anul **2024**		Anul **2025**		Anul **2026**		Anul **2027**		**TOTAL**	
	Tip[102]	Costuri medii	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 5[103] Actualizare NUI																						
NUI actualizată	Contractant			0		0		0		0,505		0,505								0		1,010
Subtotal pentru obiectivul specific nr. 5				**0**		**0**		**0**		**0,505**		**0,505**										**1,010**

– Propunerea privind EES a introdus conceptul de interfețe uniforme naționale (NUI) care urmează să fie dezvoltate și menținute de către eu-LISA. Tabelul de mai sus prevede bugetul aferent actualizării NUI pentru un tip suplimentar de schimburi de informații. Nu există costuri suplimentare aferente operațiunilor NUI, acestea fiind deja incluse în propunerea privind EES.

[102] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de stradă construiți etc.).
[103] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

A se indica obiectivele și realizările eu-LISA ⇩			Anul **2019**		Anul **2020**		Anul **2021**		Anul **2022**		Anul **2023**		Anul **2024**		Anul **2025**		Anul **2026**		Anul **2027**		**TOTAL**	
	Tip 104	Costuri medii	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 6: Reuniuni și formare																						
Reuniuni lunare privind progresele înregistrate (Dezvoltare)	0,021 pe reuniune x 10 reuniuni pe an		10	*0,210*	10	*0,210*	10	*0,210*	10	*0,210*											40	0,840
Reuniuni trimestriale (operațiuni)	0,021 x 4 reuniuni pe an		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Grupuri consultative	0,021 x 4 pe an		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Formarea SM	0,025 pe curs de formare		2	0,050	4	0,100	4	0,100	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	24	1,150
Subtotal pentru obiectivul specific nr. 6			20	**0,428**	22	**0,478**	22	**0,478**	24	**0,528**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**		**3,502**

[104] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de stradă construiți etc.).

– Subtotalul 6 include costurile aferente organizării de reuniuni de către autoritatea de management (în acest caz eu-LISA) pentru guvernanța proiectului. Acestea sunt costurile aferente unor reuniuni suplimentare pentru livrarea componentelor de interoperabilitate.

– Subtotalul 6 include costurile aferente reuniunilor eu-LISA cu personalul din statele membre care se ocupă de dezvoltarea, întreținerea și exploatarea componentelor de interoperabilitate și de organizarea și furnizarea cursurilor de formare dedicate personalului IT din statele membre.

– În timpul etapei de dezvoltare a proiectului, bugetul include 10 reuniuni pe an, iar odată încheiată etapa de pregătire a punerii în funcțiune (și anume începând cu 2019), patru reuniuni pe an. La un nivel mai înalt, se instituie încă de la început un grup consultativ, pentru a pune în practică deciziile de punere în aplicare ale Comisiei. Sunt planificate patru reuniuni pe an pentru grupurile consultative existente. De asemenea, eu-LISA pregătește și furnizează cursuri de formare destinate personalului IT din statele membre, și anume cursuri de formare privind aspectele tehnice ale componentelor de interoperabilitate.

A se indica obiectivele și realizările **eu-LISA** ⇩			Anul **2019**		Anul **2020**		Anul **2021**		Anul **2022**		Anul **2023**		Anul **2024**		Anul **2025**		Anul **2026**		Anul **2027**		**TOTAL**	
	Tip[105]	Costuri medii	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 7[106] Disponibilitate ridicată a ECRIS-TCN																						
Sistem cu disponibilitate ridicată	Configurarea sistemului			0		0		8,067												0		8,067

[105] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de stradă construiți etc.).
[106] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

Operațiuni cu disponibilitate ridicată	Sistem întreținut și exploatat		0		0		0		1,768		1,768		1,768		1,768		1,768		1,768		10,608
Subtotal pentru obiectivul specific nr. 4			**0**		**0**		**8,067**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**18,675**

– Obiectivul 7 este de a transforma ECRIS-TCN dintr-un sistem cu un grad de disponibilitate „standard” într-un sistem cu o disponibilitate ridicată. În 2021, ECRIS-TCN urmează să beneficieze de o modernizare care necesită, în esență, achiziționarea de echipamente informatice suplimentare. Întrucât se planifică ca ECRIS-TCN să fie gata în 2020, este tentant să se dezvolte acest sistem cu o disponibilitate ridicată încă de la început și să fie integrat în componentele de interoperabilitate. Cu toate acestea, având în vedere faptul că multe proiecte devin interdependente, este prudent să nu se aleagă această soluție și să se prevadă acțiuni distincte în buget. Acest buget este unul suplimentar față de costurile aferente dezvoltării, întreținerii și exploatării ECRIS-TCN în 2019 și 2020.

3.2.2.5. Impactul estimat asupra creditelor DG HOME

– ☐ 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 **DG Migrație și Afaceri Interne (DG HOME)** ⇩			Anul **2019**		Anul **2020**		Anul **2021**		Anul **2022**		Anul **2023**		Anul **2024**		Anul **2025**		Anul **2026**		Anul **2027**		**TOTAL**	
	Tip[107]	Costuri medii	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 1: Integrarea sistemelor naționale (ale statelor membre)																						
NUI gata de utilizare	Personalizarea NUI - dezvoltări						30	3,150	30	3,150											30	6,300
Sistemele statelor membre adaptate pentru interoperabilitate	Costuri de integrare						30	40,000	30	40,000	30	40,000									30	120,000

[107] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de stradă construiți etc.).

Utilizatorii finali formați	10 000 de sesiuni de formare a utilizatorilor finali la 1 000 EUR pe sesiune							5000	5,000	5000	5,000									10.000	10,000
Subtotal pentru obiectivul specific nr. 1							**43,150**		**48,150**		**45,000**										**136,300**

– Obiectivul specific nr. 1 se referă la fondurile puse la dispoziția statelor membre pentru a beneficia de sistemele centrale interoperabile. NUI este personalizată și atunci când se implementează ESP și atunci când MID devine operațional. Fiecare stat membru urmează apoi să efectueze schimbări de amploare relativ moderată (estimate la 150 de zile-om) pentru a se adapta la aceste schimburi de mesaje actualizate cu sistemele centrale. Mai substanțiale sunt costurile legate de modificarea conținutului datelor pe care o va genera interoperabilitatea și care sunt incluse în „costurile aferente integrării”. Aceste fonduri acoperă modificări privind tipul de mesaje trimise în sistemul central și procesarea răspunsului. Pentru a estima costurile acestor modificări, un buget de 4 milioane EUR este alocat fiecărui stat membru, același ca cel alocat pentru EES, întrucât volumul de muncă necesar pentru adaptarea sistemelor naționale la NUI este comparabil.

– Utilizatorii finali trebuie să fie formați pentru a putea utiliza sistemele în cauză. Aceste cursuri de formare pentru un număr mare de utilizatori finali urmează să fie finanțate la nivelul a 1 000 EUR pe sesiune, cu 10 până la 20 de utilizatori finali pentru aproximativ 10 000 de sesiuni ce urmează să fie organizate de către toate statele membre în sediile proprii.

3.2.3. Impactul estimat asupra resurselor umane

3.2.3.1. Rezumat agenția EBCG

☐ 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 **2019**	Anul **2020**	Anul **2021**	Anul **2022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**TOTAL**
Funcționari (grade AD)										
Funcționari (grade AST)	0									
Agenți contractuali	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Agenți temporari	0	0	0	0	0	0	0	0	0	0
Experți naționali detașați										
TOTAL	**0,0**	**0,0**	**0,0**	**0,350**	**1,400**	**0,233**	**0,0**	**0,0**	**0,0**	**1,983**

Activitatea preconizată a fi efectuată de către acest personal suplimentar al EBCG este limitată în timp (până în 2023), mai precis ar urma să înceapă după 24 de luni de la disponibilitatea motorului biometric pentru EES. Personalul trebuie însă recrutat în avans (s-a calculat o medie de trei luni), ceea ce explică suma prevăzută pentru 2022. După ce se încheie activitatea, sunt prevăzute sarcini de sintetizare/finalizare timp de două luni, ceea ce explică nivelul efectivelor de personal în 2024.

Nivelul personalului se bazează pe 20 de persoane necesare pentru activitatea care urmează a fi desfășurată (la care se adaugă 10 persoane furnizate de către un contractant, prevăzute în titlul 3). De asemenea, se presupune că sarcinile se îndeplinesc în cadrul unui program de lucru prelungit, și nu standard, de lucru. Se presupune că personalul de conducere și de sprijin va fi asigurat din resursele umane ale agenției.

Numărul de angajați se bazează pe ipoteza că vor trebui să fie evaluate aproximativ 550 000 de amprente digitale într-o perioadă medie de 5-10 minute pe caz (17 000 de amprente digitale verificate pe an)[108].

[108] Efectivele de personal prevăzute pentru 2020 și anii următori sunt orientative și va trebui să se stabilească dacă acestea vin sau nu în completarea previziunilor privind personalul agenției EBCG, cuprinse în COM(2015)671.

Personal	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total
Personal pentru procesarea manuală a conexiunilor şi a deciziilor	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Total titlul 1 - AC	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Total titlul 1 - AT	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Total titlul 1	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3

.

3.2.3.2. Rezumat Europol

☐ 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 **2019**	Anul **2020**	Anul **2021**	Anul **2022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**TOTAL**
Funcționari (grade AD)										
Funcționari (grade AST)	0									
Agenți contractuali	0,000	0,070	0,070	0,560	0,560	0,560	0,560	0,560	0,560	3,500
Agenți temporari	0,690	1,932	1,932	0,621	0,621	0,414	0,414	0,414	0,414	7,452
Experți naționali detașați										

TOTAL	**0,690**	**2,002**	**2,002**	**1,181**	**1,181**	**0,974**	**0,974**	**0,974**	**0,974**	**10,952**

Aceste costuri sunt estimate pe baza următoarelor efective de personal:

Numărul de ENI pentru TIC	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
Agenți contractuali	0,0	1,0	1,0	8,0	8,0	8,0	8,0	8,0	8,0	50,0
Agenți temporari	5,0	14,0	14,0	4,5	4,5	3,0	3,0	3,0	3,0	54,0
Total personal (ENI)	**5,0**	**15,0**	**15,0**	**12,5**	**12,5**	**11,0**	**11,0**	**11,0**	**11,0**	**104,0**

Pentru Europol se prevede personal suplimentar în domeniul TIC pentru a se consolida sistemele de informații ale agenției astfel încât să facă față creșterii numărului de interogări din ESP și ETIAS și, ulterior, pentru a se asigura întreținerea sistemelor 24 de ore din 24, șapte zile din șapte.

– Pentru faza de implementare a ESP (în 2020 și 2021), este nevoie de experți tehnici suplimentari (arhitecți, ingineri, dezvoltatori, testeri). În 2022 și anii următori va fi nevoie de un număr redus de experți tehnici pentru a implementa restul componentelor de interoperabilitate și a întreține sistemele.

– Începând cu a doua jumătate a anului 2021 trebuie pus în practică un sistem TIC de monitorizare 24 de ore din 24, șapte zile din șapte, pentru a se asigura nivelurile operaționale pentru ESP și ETIAS. Acest lucru va fi asigurat de doi agenți contractuali, care vor lucra în 4 schimburi, 24 de ore din 24, șapte zile din șapte.

– În măsura posibilului, profilurile au fost împărțite între agenți temporari și agenți contractuali. Trebuie să se țină cont de faptul că, din cauza nivelului ridicat al cerințelor de securitate, în anumite posturi pot fi angajați numai agenți temporari. Cererea de agenți temporari va ține seama de rezultatele procedurii de conciliere din cadrul procedurii bugetare 2018.

3.2.3.3. Rezumat CEPOL

☐ 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 **2019**	Anul **2020**	Anul **2021**	Anul **2022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**TOTAL**
Funcționari (grade AD)										
Funcționari (grade AST)										
Agenți contractuali			0,070	0,070						**0,140**
Agenți temporari		0,104	0,138	0,138	0,138	0,138	0,138	0,138	0,138	1,070
Experți naționali detașați										
TOTAL		**0,104**	**0,208**	**0,208**	**0,138**	**0,138**	**0,138**	**0,138**	**0,138**	**1,210**

Este necesar să se prevadă personal suplimentar întrucât cursurile de formare a formatorilor din statele membre trebuie să fie elaborate în mod specific în vederea utilizării componentelor de interoperabilitate în circumstanțe operaționale.

- Elaborarea programei de formare și a unor module de formare ar trebui să înceapă cu cel puțin 8 luni înainte ca sistemul să devină operațional. Cursurile de formare vor avea cea mai mare frecvență în primii doi ani după ce sistemul va deveni operațional. Cu toate acestea, pe baza experienței acumulate în cursul implementării Sistemul de informații Schengen, este necesar ca aceste cursuri

să fie menținute pe o perioadă de timp mai îndelungată pentru a se asigura o punere în aplicare coerentă.

- este nevoie de personal suplimentar pentru elaborarea, coordonarea și punerea în aplicare a programei de formare, a cursurilor desfășurate în centre de formare externe și a cursurilor online. Aceste cursuri pot fi oferite exclusiv ca o completare a catalogului de formare existent al CEPOL și, prin urmare, este nevoie de personal suplimentar.

- Se preconizează ca un agent temporar să aibă rolul de administrator de formare pe tot parcursul perioadei de dezvoltare și întreținere, care să fie sprijinit de un agent contractual în perioada cea mai intensă a organizării cursurilor de formare.

3.2.3.4. Rezumat eu-LISA

☐ 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 **2019**	Anul **2020**	Anul **2021**	Anul **2022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**TOTAL**
Funcționari (grade AD)										
Funcționari (grade AST)										
Agenți contractuali	0,875	1,400	1,855	2,555	2,415	2,170	2,100	2,100	2,100	17,570
Agenți temporari	2,001	3,450	4,347	4,347	4,209	3,312	3,036	3,036	3,036	30,774
Experți naționali detașați										
TOTAL	**2,876**	**4,850**	**6,202**	**6,902**	**6,624**	**5,482**	**5,136**	**5,136**	**5,136**	**48,344**

– Cerințele în materie de personal țin seama de faptul că cele patru componente și CRRS constituie un portofoliu de proiecte interdependente (și anume un program). Pentru a gestiona interdependențele dintre proiecte, se creează o echipă de conducere a programului, care cuprinde managerii de program și de proiect și profilurile (adesea denumite arhitecți) care trebuie să definească elementele comune ale acestora. Realizarea programului/proiectului necesită, de asemenea, profiluri pentru suportul tehnic aferent.

– Cerințele în materie de personal pentru fiecare proiect au fost estimate prin analogie cu proiectele anterioare (Sistemul de informații privind vizele), făcându-se distincție între faza de execuție și faza operațională.

– Profilurile care trebuie să rămână în faza de exploatare sunt recrutate ca agenți temporari. Profilurile necesare pe parcursul executării programului/proiectului sunt recrutate ca agenți

contractuali. Pentru a se asigura continuitatea preconizată a sarcinilor și pentru a menține expertiza în cadrul agenției, numărul de posturi este împărțit în proporții aproape egale între agenții temporari și agenții contractuali.

– Se pornește de la ipoteza că nu va mai fi nevoie de personal suplimentar pentru a realiza proiectul ECRIS-TCN cu o disponibilitate ridicată și că pentru personalul eu-LISA care va fi dedicat proiectului se va reutiliza personalul existent care lucrează la proiectele care se vor încheia în acea perioadă de timp.

Aceste estimări se bazează pe următoarea schemă de personal:

pentru agenți contractuali:

3.2.1. Realizări EU-LISA (egal cu T1) ca număr de persoane	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total (formulă)
Agenți contractuali										-
Gestionare program/proiect	4,0	5,0	5,5	5,5	4,5	3,0	3,0	3,0	3,0	36,5
CRRS PM	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*1,5*
MID	*0,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*2,0*
Birou program/proiect	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*14,0*
Asigurarea calității	*1,0*	*2,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*19,0*
Financiar și achiziții	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Gestionare financiară										*0,0*
Planificare bugetară și control										*0,0*
Gestionare achiziții/contracte	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Experți tehnici	7,0	7,0	7,0	7,0	6,0	5,0	5,0	5,0	5,0	54,0
CRRS	*3,0*	*3,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*22,0*
ESP	*4,0*	*4,0*	*4,0*	*4,0*	*4,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
BMS comun	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Testare	1,5	3,0	4,0	4,0	4,0	3,0	2,0	2,0	2,0	25,5
CRRS	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*6,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
BMS comun	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,5*	*1,0*	*2,0*	*2,5*	*2,5*	*1,5*	*1,0*	*1,0*	*1,0*	*13,0*
MID	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*6,5*
Monitorizarea sistemului	0,0	5,0	10,0	20,0	20,0	20,0	20,0	20,0	20,0	135,0
Comun (24:7)	0,0	*5,0*	*10,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*135,0*
Coordonare generală	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Resurse umane	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
RU	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Subtotal personal contractual	**12,5**	**20,0**	**26,5**	**36,5**	**34,5**	**31,0**	**30,0**	**30,0**	**30,0**	**251,0**

pentru agenți temporari:

Agenți temporari										
Gestionare program/proiect	3,0	4,0	5,5	5,5	5,5	4,5	4,0	4,0	4,0	40,0
Gestionare program	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Gestionare proiect	*0,0*	*0,0*	*1,0*	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*12,0*
Birou program/proiect	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
ESP	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
BMS comun	*0,5*	*0,5*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*4,0*
CIR	*0,0*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Financiar și achiziții	3,0	3,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	34,0
Gestionare financiară	*0,0*	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*7,0*
Planificare bugerată și control	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Gestionare achiziții/contracte	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*18,0*
Experți tehnici	6,0	14,0	17,0	17,0	15,0	11,0	10,0	10,0	10,0	110,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
BMS comun	*2,0*	*3,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
CIR	*2,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Securitate	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*17,0*
MID	*0,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*12,0*
Architecți	*1,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,0*	*1,0*	*1,0*	*17,0*
Testare	2,5	3,0	4,0	4,0	4,0	2,5	2,0	2,0	2,0	26,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,5*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*6,5*
BMS comun	*2,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,5*	*1,5*	*1,5*	*19,5*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Monitorizarea sistemului	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
BMS comun	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Formare	0,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	8,0
formare	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*8,0*
Resurse umane	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
RU	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Altele	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	5,0
Specialist în protecția datelor	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	*5,0*
Subtotal agenți temporari	**14,5**	**25,0**	**31,5**	**31,5**	**30,5**	**24,0**	**22,0**	**22,0**	**22,0**	**223,0**
Total	**27,0**	**45,0**	**58,0**	**68,0**	**65,0**	**55,0**	**52,0**	**52,0**	**52,0**	**474,0**

3.2.4. Impactul estimat asupra creditelor cu caracter administrativ

3.2.4.1. DG HOME 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 **2019**	Anul **2020**	Anul **2021**	Anul **2022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**TOTAL**
RUBRICA 5 din cadrul financiar multianual										
Resurse umane DG HOME	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Alte cheltuieli administrative	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
Subtotal RUBRICA 5 din cadrul financiar multianual	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

În afara RUBRICII 5[109] **din cadrul financiar multianual**	(Neutilizat)									
Resurse umane										
Alte cheltuieli cu caracter administrativ										
Subtotal În afara RUBRICII 5 din cadrul financiar multianual										

TOTAL	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

.

[109] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

3.2.4.2. Necesarul de resurse umane estimat

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane.

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

Estimări în echivalent normă întreagă

	Anul **2019**	Anul **2020**	Anul **2021**	Anul **2022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**TOTAL**
• **Posturi din schema de personal (funcționari și agenți temporari)**										
18 01 01 01 (la sediu și în birourile de reprezentare ale Comisiei) DG HOME	5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0
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)**[110]										
XX 01 02 02 (AC, AL, END, INT și JED în delegații)										
XX 01 04 **yy** [111] - la sediu										
XX 01 04 **yy** [111] - în delegații										
XX 01 05 02 (AC, END, INT - cercetare indirectă)										
10 01 05 02 (AC, END, INT - cercetare directă)										
Alte linii bugetare (a se preciza)										
TOTAL	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**2,0**	**2,0**	**2,0**	**36,0**

18 este domeniul de politică sau titlul din buget în cauză.

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau realocate intern în cadrul DG-ului, completate, după caz, prin resurse suplimentare ce ar putea fi alocate DG-ului care gestionează acțiunea în cadrul procedurii de alocare anuală și în lumina constrângerilor bugetare.

Descrierea sarcinilor care trebuie efectuate:

Monitorizarea proiectului și măsuri subsecvente. Trei funcționari pentru luarea de măsuri subsecvente. Personalul care se ocupă de preluarea atribuțiilor Comisiei în ceea ce privește livrarea programului: verificarea conformității față de propunerea legislativă, abordarea aspectelor legate de conformitate, elaborarea unor rapoarte adresate Parlamentului European și Consiliului, evaluarea progreselor înregistrate de statele membre. Întrucât acest program reprezintă o activitate suplimentară față de volumul de lucru existent, este nevoie de personal suplimentar. Această creștere de personal este limitată în timp și acoperă doar perioada de dezvoltare.

Gestionarea UMF

Comisia va gestiona standardul UMF zilnic. Este nevoie de doi funcționari în acest scop: o persoană ca expert în materie de asigurare a respectării legii și o altă persoană care să cunoască bine modelarea operațională, precum și să aibă cunoștințe în domeniul TIC.

Formatul universal de mesaje (UMF) stabilește un standard pentru schimburile structurate transfrontaliere de informații între sistemele de informații, autoritățile și/sau organizațiile din domeniul justiției și afacerilor interne. UMF definește

[110] AC = agent contractual; AL = agent local; END= expert național detașat; INT = personal pus la dispoziție de agenții de muncă temporară; JED = expert tânăr în delegații.

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

un vocabular comun și structuri logice pentru informațiile care fac frecvent obiectul schimburilor, cu scopul de a facilita interoperabilitatea, permițând crearea și citirea conținutului în mod coerent și cu asigurarea echivalenței semantice.

În vederea asigurării unor condiții uniforme pentru punerea în aplicare a formatului universal de mesaje, se propune conferirea competențelor de executare Comisiei. Se propune ca aceste competențe să fie exercitate în conformitate cu 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.

3.2.5. Compatibilitatea cu actualul cadru financiar multianual

– ☐ Propunerea/inițiativa este compatibilă cu cadrul financiar multianual existent.

– ☒ Propunerea/inițiativa necesită o reprogramare a rubricii corespunzătoare din cadrul financiar multianual.

A se explica reprogramarea necesară, precizându-se liniile bugetare în cauză și sumele aferente.

Regulamentul de instituire în cadrul FSI a sprijinului pentru frontiere este instrumentul financiar în care a fost inclus bugetul alocat punerii în aplicare a inițiativei privind interoperabilitatea.

În regulamentul respectiv, la articolul 5 litera (b) se prevede suma de 791 de milioane EUR pentru dezvoltarea de sisteme informatice ce au la bază sisteme informatice existente și/sau noi de sprijin pentru gestionarea fluxurilor migratorii la frontierele externe, sub rezerva adoptării actelor legislative relevante ale Uniunii și cu respectarea condițiilor prevăzute la articolul 15. Din cele 791 de milioane EUR, 480,2 milioane EUR sunt rezervate dezvoltării EES, 210 milioane EUR dezvoltării ETIAS și 67,9 milioane EUR revizuirii SIS II. Restul (32,9 milioane EUR) va fi realocat folosind mecanismele ISF-B. **Propunerea de față solicită 32,1 milioane EUR pentru actuala perioadă a CFM, care se încadrează în bugetul restant.**

Concluzia din caseta de mai sus cu privire la suma necesară de 32,1 milioane EUR este rezultatul următoarei foi de calcul:

ANGAJAMENTE										
3.2. Impactul estimat asupra cheltuielilor DG HOME										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (oriz.)**
18 02 01 03 - Frontiere inteligente (include sprijinul către SM)	0	0	43,150	48,150	45,000	0	0	0	0	136,300
Total (1)	**0**	**0**	**43,150**	**48,150**	**45,000**	**0**	**0**	**0**	**0**	**136,300**
18,0207 -3.2. eu-LISA										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (formulă)**
T1: Cheltuieli cu personalul	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
T2: Cheltuieli de infrastructură și de funcționare	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
T3: Cheltuieli operaționale	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Total (2)	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**
		22,861							**202,181**	**225,041**
18.02.04 -3.2. Europol										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (formulă)**
T1: Cheltuieli cu personalul	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
T2: Cheltuieli de infrastructură și de funcționare	0	0	0	0	0	0	0	0	0	0
T3: Cheltuieli operaționale	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
Total (3)	**0,690**	**8,382**	**8,382**	**3,589**	**3,589**	**3,382**	**8,732**	**8,732**	**3,382**	**48,860**
		9,072							39,788	48,860
18.02.05 -3.2. CEPOL										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (formulă)**
T1: Cheltuieli cu personalul	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
T2: Cheltuieli de infrastructură și de funcționare	0	0	0	0	0	0	0	0	0	0
T3: Cheltuieli operaționale	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Total (4)	**0**	**0,144**	**0,384**	**0,482**	**0,208**	**0,208**	**0,208**	**0,208**	**0,208**	**2,050**
		0,144							**1,906**	**2,050**
18.02.0 -3.2. Frontex - EBCG										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (formulă)**
T1: Cheltuieli cu personalul	0	0	0	0,350	1,400	0,233	0	0	0	1,983
T2: Cheltuieli de infrastructură și de funcționare	0	0	0	0,075	0,300	0,050	0	0	0	0,425
T3: Cheltuieli operaționale	0	0	0	0,183	2,200	0	0	0	0	2,383
Total (5)	**0**	**0**	**0**	**0,608**	**3,900**	**0,283**	**0**	**0**	**0**	**4,792**
		0							**4,792**	**4,792**
TOTAL (1)+(2)+(3) +(4) +(5)	6,520	25,556	103,659	97,578	82,350	24,243	27,549	27,469	22,119	417,043
		32,076							384,966	
3.2. DG HOME Rubrica 5 „Cheltuieli administrative”										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
Total (6)	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695
TOTAL (1)+(2)+(3)+(4)+(5)+(6)	7,533	26,569	104,672	98,591	83,363	25,256	28,088	28,008	22,658	424,738

– ☐ Propunerea/inițiativa necesită recurgerea la instrumentul de flexibilitate sau la revizuirea cadrului financiar multianual.

3.2.6. Contribuția terților

– Propunerea/inițiativa **nu** prevede cofinanțare din partea terților.

3.3. Impactul estimat asupra veniturilor

– ☐ Propunerea/inițiativa nu are impact financiar asupra veniturilor.

– ☒ Propunerea/inițiativa are următorul impact financiar:

– – ☐ asupra resurselor proprii

– – ☒ asupra veniturilor diverse

milioane EUR (cu trei zecimale)

Linia bugetară pentru venituri:	Credite disponibile pentru exercițiul financiar în curs	Impactul propunerii/inițiativei[112]								
		Anul **2019**	Anul **2020**	Anul **2021**	Anul **2022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**
Articolul 6313 - Alte contribuții în cadrul acquis-ului Schengen (CH, NO, LI și IS)……		pm	pm	pm	pm	pm	pm	pm	pm	pm

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

18.0207

A se preciza metoda de calcul a impactului asupra veniturilor.

Bugetul include o contribuție din partea țărilor asociate la punerea în practică, aplicarea și dezvoltarea acquis-ului Schengen și la măsurile referitoare la Eurodac prevăzute de acordurile respective.

[112] În ceea ce privește resursele proprii tradiționale (taxe vamale, cotizații pentru zahăr), sumele indicate trebuie să fie sume nete, și anume sume brute după deducerea unei cote de 25 % pentru costurile de colectare.