COMISIA
EUROPEANĂ

Bruxelles, 21.12.2016
COM(2016) 882 final

2016/0408 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Regulamentului (UE) nr. 515/2014 și de abrogare a Regulamentului (CE) nr. 1987/2006

EXPUNERE DE MOTIVE

1. CONTEXT

• Temeiurile și obiectivele propunerii

În ultimii doi ani, Uniunea Europeană a depus eforturi pentru abordarea simultană a provocărilor distincte legate de gestionarea migrației, gestionarea integrată a frontierelor externe ale UE și combaterea terorismului și a criminalității transfrontaliere. Schimbul eficace de informații dintre statele membre, precum și dintre statele membre și agențiile relevante ale UE este esențial pentru a oferi un răspuns solid la aceste provocări și a construi o uniune a securității efectivă și autentică.

Sistemul de informații Schengen (SIS) este cel mai de succes instrument pentru cooperarea eficace a autorităților din domeniul imigrației, polițienești, vamale și judiciare din UE și din țările asociate spațiului Schengen. Autoritățile competente din statele membre, cum ar fi poliția, polițiștii de frontieră și lucrătorii vamali, trebuie să aibă acces la informații de înaltă calitate cu privire la persoanele sau obiectele pe care le controlează și să dispună de instrucțiuni clare cu privire la ceea ce trebuie făcut în fiecare caz. Acest sistem de informații la scară largă este un element central al cooperării Schengen și joacă un rol crucial în facilitarea liberei circulații a persoanelor în spațiul Schengen. SIS permite autorităților competente să introducă și să consulte date privind persoane căutate, persoane suspectate de a nu avea dreptul de intrare sau de ședere în UE, persoane dispărute - în special copii - și obiecte care este posibil să fi fost furate, însușite în mod ilegal sau pierdute. Pe lângă informații referitoare la o anumită persoană sau un anumit obiect, SIS conține și instrucțiuni clare pentru autoritățile competente cu privire la ceea ce trebuie să facă după găsirea respectivei persoane sau a respectivului obiect.

În 2016, Comisia a efectuat o evaluare cuprinzătoare a SIS[1], la trei ani după intrarea în funcțiune a sistemului de a doua generație. Această evaluare a arătat că SIS a fost un autentic succes operațional. În 2015, autoritățile naționale competente au verificat persoane și obiecte prin consultarea datelor din SIS în aproape 2,9 miliarde de cazuri și au făcut schimb de peste 1,8 milioane de informații suplimentare. Cu toate acestea, după cum s-a anunțat în Programul de lucru al Comisiei pentru 2017, pe baza acestei experiențe pozitive, eficacitatea și eficiența sistemului ar trebui consolidate în continuare. În acest scop, Comisia prezintă un prim set de trei propuneri pentru a îmbunătăți și a extinde utilizarea SIS ca urmare a evaluării, continuându-și, în același timp, activitatea care vizează creșterea interoperabilității sistemelor existente și viitoare de asigurare a respectării legii și de gestionare a frontierelor, pe baza lucrărilor în curs ale Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate.

Aceste propuneri vizează utilizarea sistemului (a) pentru gestionarea frontierelor, (b) pentru cooperarea polițienească și cooperarea judiciară în materie penală și (c) pentru returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală. Primele două propuneri formează împreună temeiul juridic pentru instituirea, funcționarea și utilizarea SIS. Propunerea de utilizare a SIS pentru returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală

[1] Raportul către Parlamentul European și Consiliu privind evaluarea Sistemului de informații Schengen de a doua generație (SIS II) în conformitate cu articolul 24 alineatul (5), articolul 43 alineatul (3) și articolul 50 alineatul (5) din Regulamentul (CE) nr. 1987/2006 și cu articolul 59 alineatul (3) și articolul 66 alineatul (5) din Decizia 2007/533/JAI și documentul de lucru însoțitor (JO…).

completează propunerea privind gestionarea frontierelor și dispozițiile conținute de aceasta, stabilind o nouă categorie de semnalări și contribuind la punerea în aplicare și la monitorizarea Directivei 2008/115/CE[2].

Dată fiind geometria variabilă în ceea ce privește participarea statelor membre la politicile UE din spațiul de libertate, securitate și justiție, este necesar să se adopte trei instrumente juridice separate care vor conlucra însă în mod sinergic pentru a permite funcționarea și utilizarea cuprinzătoare a sistemului.

În paralel, în vederea consolidării și a îmbunătățirii gestionării informațiilor la nivelul UE, în aprilie 2016 Comisia a inițiat un proces de reflecție cu privire la „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”[3]. Obiectivul principal este asigurarea faptului că autoritățile competente dispun în mod sistematic de datele necesare din diferitele sisteme de informații. În vederea realizării acestui obiectiv, Comisia a reexaminat actuala arhitectură din domeniul informațiilor pentru a identifica deficiențele și lacunele generate de carențele funcționalităților sistemelor existente, precum și de fragmentarea arhitecturii globale a UE în materie de gestionare a datelor. În sprijinul acestei activități, Comisia a înființat un Grup de experți la nivel înalt pentru sistemele de informații și interoperabilitate, ale cărui constatări intermediare au stat, de asemenea, la baza acestui prim set de propuneri în ceea ce privește aspectele legate de calitatea datelor[4]. În discursul președintelui Juncker privind starea Uniunii din septembrie 2016 s-a menționat, de asemenea, importanța eliminării deficiențelor actuale în materie de gestionare a informațiilor și a îmbunătățirii interoperabilității și a interconectării între sistemele de informații existente.

În urma constatărilor Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate, care vor fi prezentate în primul semestru al anului 2017, Comisia va lua în considerare, la jumătatea anului 2017, un al doilea set de propuneri pentru îmbunătățirea în continuare a interoperabilității SIS cu alte sisteme informatice. Revizuirea Regulamentului (UE) nr. 1077/2011[5] privind Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA) este un element la fel de important al acestor lucrări și probabil va face obiectul unor propuneri separate ale Comisiei, tot în 2017. Investirea într-un schimb de informații și într-o gestionare a informațiilor rapide, eficace și calitative și asigurarea interoperabilității bazelor de date și a sistemelor de informații ale UE constituie un aspect important al abordării actualelor provocări în materie de securitate.

Cadrul juridic actual al SIS de a doua generație - în ceea ce privește utilizarea acestuia în scopul verificărilor la frontiere asupra resortisanților țărilor terțe - se bazează pe un instrument

---

2 Directiva 2008/115/CE a Parlamentului European și a Consiliului din 16 decembrie 2008 privind standardele și procedurile comune aplicabile în statele membre pentru returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală (JO L 348, 24.12.2008, p. 98).

3 COM(2016) 205 final, 6.4.2016.

4 Decizia 2016/C 257/03 a Comisiei din 17.6.2016.

5 Regulamentul (UE) nr. 1077/2011 al Parlamentului European și al Consiliului din 25 octombrie 2011 de instituire a Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (JO L 286, 1.11.2011, p. 1).

aferent fostului prim pilon, și anume Regulamentul (CE) nr. 1987/2006[6]. Prezenta propunere înlocuiește[7] actualul instrument juridic pentru:

- a impune statelor membre obligația de a introduce o semnalare în SIS în toate cazurile în care pentru un resortisant al unei țări terțe aflat în situație de ședere ilegală s-a emis o interdicție de intrare în conformitate cu dispoziții care respectă Directiva 2008/115/CE;
- a armoniza procedurile naționale de utilizare a SIS în ceea ce privește procedura de consultare pentru a evita ca un resortisant al unei țări terțe care face obiectul unei interdicții de intrare să dețină un permis de ședere valabil eliberat de un stat membru;
- a introduce modificări tehnice cu scopul de a îmbunătăți securitatea și a contribui la reducerea sarcinii administrative;
- a aborda utilizarea completă a SIS de la un capăt la altul (*end-to-end*), care include nu numai sistemul central și sistemele naționale, ci și nevoile utilizatorilor finali prin asigurarea faptului că aceștia primesc toate datele necesare pentru a-și îndeplini sarcinile și respectă toate normele de securitate atunci când prelucrează date din SIS.

Propunerile dezvoltă și îmbunătățesc sistemul existent, nu instituie unul nou. Revizuirea SIS va sprijini și va consolida acțiunile Uniunii Europene prevăzute în cadrul Agendei europene privind migrația și pune în aplicare:

(1) consolidarea rezultatelor lucrărilor privind punerea în aplicare a SIS desfășurate în ultimii trei ani care implică modificări tehnice ale SIS central pentru a extinde anumite categorii de semnalări existente și a furniza funcționalități noi;

(2) recomandările privind modificările tehnice și procedurale care rezultă dintr-o evaluare cuprinzătoare a SIS[8];

(3) solicitările privind îmbunătățiri tehnice primite din partea utilizatorilor finali ai SIS și

(4) constatările provizorii ale Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate[9] în ceea ce privește calitatea datelor.

Având în vedere faptul că prezenta propunere este strâns legată de Propunerea Comisiei de regulament privind instituirea, funcționarea și utilizarea SIS în domeniul cooperării polițienești și al cooperării judiciare în materie penală, o serie de dispoziții sunt comune ambelor texte. Printre acestea se numără măsuri referitoare la utilizarea SIS de la un capăt la altul, care includ nu numai funcționarea sistemului central și a sistemelor naționale, ci și nevoile utilizatorilor finali, măsuri consolidate pentru asigurarea continuității activității, măsuri privind calitatea datelor, protecția datelor și securitatea datelor, precum și dispoziții

---

6 Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație (SIS II) (JO L 381, 28.12.2006, p. 4).

7 A se vedea secțiunea 2 intitulată „Alegerea instrumentului” în care se explică de ce s-a optat pentru o înlocuire, mai degrabă decât pentru o reformare a legislației actuale.

8 Raportul către Parlamentul European și Consiliu privind evaluarea Sistemului de informații Schengen de a doua generație (SIS II) în conformitate cu articolul 24 alineatul (5), articolul 43 alineatul (3) și articolul 50 alineatul (5) din Regulamentul (CE) nr. 1987/2006 și cu articolul 59 alineatul (3) și articolul 66 alineatul (5) din Decizia 2007/533/JAI și documentul de lucru însoțitor (JO…).

9 Grupul de experți la nivel înalt - Raportul președintelui din 21 decembrie 2016.

privind măsuri de monitorizare, de evaluare și de raportare. Ambele propuneri extind, de asemenea, utilizarea informațiilor biometrice[10].

Odată cu escaladarea crizei migrației și a refugiaților în 2015, a sporit în mod considerabil necesitatea de a lua măsuri eficace pentru a combate migrația neregulamentară. În *Planul de acțiune al UE privind returnarea*[11] pe care l-a elaborat, Comisia a anunțat că va propune ca statele membre să aibă obligația de a introduce în SIS toate interdicțiile de intrare pentru a contribui la prevenirea reintrării în spațiul Schengen a resortisanților țărilor terțe care nu au dreptul de intrare și de ședere pe teritoriul statelor membre. Interdicțiile de intrare emise în conformitate cu dispoziții care respectă Directiva 2008/115/CE au efect în întreg spațiul Schengen; prin urmare, autoritățile unui alt stat membru decât cel care a emis interdicția pot avea, de asemenea, competența de a asigura respectarea acesteia la frontierele externe. Regulamentul (CE) nr. 1987/2006 existent doar permite, dar nu impune, statelor membre să introducă în SIS semnalări privind refuzul intrării și al șederii pe baza interdicțiilor de intrare. Prin impunerea obligației de a introduce în SIS toate interdicțiile de intrare se poate realiza un nivel mai ridicat de eficacitate și de armonizare.

- **Coerența cu alte politici ale Uniunii, precum și cu instrumentele juridice existente și viitoare**

Prezenta propunere este pe deplin coerentă cu dispozițiile Directivei 2008/115/CE privind emiterea și asigurarea respectării interdicțiilor de intrare și este pe deplin aliniată la aceste dispoziții. Prin urmare, prezenta propunere completează dispozițiile existente privind interdicțiile de intrare și contribuie la asigurarea respectării efective a acestor interdicții la frontiera externă, facilitând aplicarea obligațiilor definite în Directiva privind returnarea și prevenind cu succes reintrarea resortisanților țărilor terțe în cauză în spațiul Schengen.

- **Coerența cu alte domenii de politică a Uniunii**

Prezenta propunere este strâns legată de alte politici ale Uniunii, pe care le completează, și anume:

(1) **securitatea internă,** în ceea ce privește rolul SIS de prevenire a intrării resortisanților țărilor terțe care reprezintă o amenințare la adresa securității;

(2) **protecția datelor**, în măsura în care prezenta propunere asigură protecția drepturilor fundamentale ale persoanelor ale căror date cu caracter personal sunt prelucrate în SIS.

(3) Prezenta propunere este, de asemenea, strâns legată de alte acte legislative ale Uniunii, pe care le completează, și anume cele referitoare la:

(4) **gestionarea frontierelor externe**, în măsura în care prezenta propunere acordă sprijin statelor membre pentru controlarea părții lor din frontierele externe ale UE și pentru întărirea eficacității sistemului UE de controale la frontierele externe;

(5) o **politică de returnare** eficace **a UE**, care contribuie la sistemul UE de depistare și prevenire a reintrării resortisanților țărilor terțe după returnarea lor și care întărește acest sistem. Prezenta propunere va contribui la reducerea stimulentelor pentru

[10] Pentru o explicație detaliată a modificărilor incluse în prezenta propunere, a se vedea secțiunea 5 intitulată „Elemente diverse”.

[11] COM(2015) 453 final.

migrația neregulamentară către UE, unul dintre principalele obiective ale Agendei europene privind migrația[12];

(6) **Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă**, în ceea ce privește (i) posibilitatea ca personalul agenției să efectueze analize ale riscurilor și (ii) accesul la SIS al unității centrale a ETIAS din cadrul agenției în scopurile utilizării sistemului european de informații și de autorizare privind călătoriile (ETIAS)[13] propus, precum și (iii) furnizarea unei interfețe tehnice care să asigure accesul la SIS al echipelor europene de poliție de frontieră și gardă de coastă, al echipelor personalului implicat în sarcini legate de returnare și al membrilor echipelor de sprijin pentru gestionarea migrației pentru ca, în limitele mandatului lor, acestea să aibă dreptul de a accesa și de a efectua căutări în datele introduse în SIS;

(7) **Europol** - se propun drepturi mai ample de acces la datele din SIS și de efectuare de căutări în aceste date, în limitele mandatului său.

Prezenta propunere este, de asemenea, strâns legată de o serie de instrumente legislative viitoare ale Uniunii, pe care le completează, și anume cele referitoare la:

(8) **sistemul de intrare/ieșire,** care a propus o combinație de amprente digitale și imagini faciale ca elemente biometrice de identificare pentru funcționarea sistemului de intrare/ieșire (EES); prezenta propunere urmărește să reflecte această abordare;

(9) **ETIAS,** care a propus o evaluare aprofundată în materie de securitate, inclusiv o verificare în SIS, a resortisanților țărilor terțe exonerați de obligația de a deține viză care intenționează să călătorească în UE.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

• Temeiul juridic

Prezenta propunere utilizează articolul 77 alineatul (2) literele (b) și (d), precum și articolul 79 alineatul (2) litera (c) din Tratatul privind funcționarea Uniunii Europene ca temei juridic pentru dispozițiile din domeniul gestionării integrate a frontierelor și al imigrației ilegale.

• Geometrie variabilă

Prezenta propunere constituie o dezvoltare a acquis-ului Schengen privind verificările la frontiere. Prin urmare, trebuie luate în considerare următoarele consecințe care rezultă din diferitele protocoale și acorduri cu țările asociate:

Danemarca: în conformitate cu articolul 4 din Protocolul nr. 22 privind poziția Danemarcei anexat la tratate, Danemarca decide, în termen de șase luni de la data la care Consiliul a decis cu privire la prezentul regulament, dacă va transpune în legislația sa internă prezenta propunere, care dezvoltă acquis-ul Schengen.

Regatul Unit și Irlanda: în conformitate cu articolele 4 și 5 din Protocolul privind integrarea acquis-ului Schengen în cadrul Uniunii Europene și în conformitate cu 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 și cu Decizia 2002/192/CE a Consiliului din 28 februarie 2002 privind solicitarea Irlandei de a participa la

[12] COM(2015) 240 final.
[13] COM(2016) 731 final.

unele dintre dispozițiile acquis-ului Schengen, Regatul Unit și Irlanda nu participă la Regulamentul (UE) 2016/399 (Codul frontierelor Schengen), nici la alte instrumente juridice cunoscute în mod obișnuit sub denumirea de „acquis-ul Schengen”, și anume instrumentele juridice care organizează și susțin eliminarea controalelor la frontierele interne și alte măsuri de însoțire privind controalele la frontierele externe. Prezentul regulament constituie o dezvoltare a acestui acquis și, prin urmare, Regatul Unit și Irlanda nu participă la adoptarea prezentului regulament, nu au obligații în temeiul acestuia și nu fac obiectul aplicării sale.

Bulgaria și România: prezentul regulament constituie un act care se întemeiază pe acquis-ul Schengen sau care este conex acestuia în sensul articolului 4 alineatul (2) din Actul de aderare din 2005. Prezentul regulament trebuie coroborat cu Decizia 2010/365/UE a Consiliului din 29 iunie 2010[14] prin care au devenit aplicabile în Bulgaria și în România, sub rezerva anumitor restricții, dispozițiile acquis-ului Schengen referitoare la Sistemul de informații Schengen.

Cipru și Croația: prezentul regulament constituie un act care se întemeiază pe acquis-ul Schengen sau care este conex acestuia, în sensul articolului 3 alineatul (2) din Actul de aderare din 2003, și, respectiv, al articolului 4 alineatul (2) din Actul de aderare din 2011.

Țările asociate: pe baza acordurilor respective de asociere a acestor țări în vederea punerii în aplicare, a asigurării respectării și a dezvoltării acquis-ului Schengen, Islanda, Norvegia, Elveția și Liechtenstein au obligații în temeiul regulamentului propus.

- **Subsidiaritatea**

Prezenta propunere se bazează pe actualul SIS, care este în funcțiune din 1995, și îl va dezvolta. Cadrul interguvernamental inițial a fost înlocuit de instrumente ale Uniunii la 9 aprilie 2013 [Regulamentul (CE) nr. 1987/2006 și Decizia 2007/533/JAI a Consiliului]. O analiză completă a subsidiarității a fost efectuată în alte ocazii; prezenta inițiativă urmărește să îmbunătățească în continuare dispozițiile existente, să elimine lacunele identificate și să amelioreze procedurile operaționale.

Acest nivel considerabil de schimb de informații între statele membre nu poate fi realizat prin soluții descentralizate. Având în vedere amploarea, efectele și impacturile acțiunii, prezenta propunere poate fi realizată mai bine la nivelul Uniunii.

Printre obiectivele prezentei propuneri se numără și îmbunătățiri tehnice menite să sporească eficiența SIS, precum și eforturi de armonizare a utilizării sistemului în toate statele membre participante. Ca urmare a caracterului transnațional al acestor obiective și a provocărilor aferente asigurării unui schimb eficace de informații pentru combaterea amenințărilor care se diversifică tot mai mult, UE este în măsură să propună soluții la aceste probleme, care nu pot fi realizate într-o măsură suficientă de statele membre în mod individual.

Dacă nu se remediază limitările existente ale SIS, există riscul ca numeroase oportunități pentru maximizarea eficienței și a valorii adăugate a UE să fie ratate și să existe unghiuri moarte care să împiedice activitatea autorităților competente. De exemplu, lipsa unor norme armonizate privind ștergerea semnalărilor redundante din sistem poate conduce la împiedicarea liberei circulații a persoanelor, care este un principiu fundamental al Uniunii.

[14] Decizia 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).

- **Proporționalitatea**

Articolul 5 din Tratatul privind Uniunea Europeană prevede că acțiunea Uniunii nu depășește ceea ce este necesar pentru realizarea obiectivelor stabilite în tratat. Forma aleasă pentru această acțiune a UE trebuie să permită propunerii să își atingă obiectivul și să fie pusă în aplicare în modul cel mai eficace posibil. Inițiativa propusă constituie o revizuire a SIS în ceea ce privește verificările la frontiere.

Propunerea se bazează pe principiile luării în considerare a vieții private începând cu momentul conceperii. În ceea ce privește dreptul la protecția datelor cu caracter personal, prezenta propunere este proporțională, deoarece prevede norme specifice privind ștergerea unei semnalări și nu prevede colectarea și stocarea datelor o perioadă mai îndelungată decât este absolut necesar pentru a permite sistemului să funcționeze și să își îndeplinească obiectivele. Semnalările SIS conțin numai date care sunt necesare pentru a identifica și a localiza o persoană sau un obiect și pentru a permite întreprinderea acțiunii operaționale corespunzătoare. Toate celelalte detalii suplimentare sunt furnizate prin intermediul birourilor SIRENE, care asigură efectuarea schimbului de informații suplimentare.

În plus, propunerea prevede punerea în aplicare a tuturor garanțiilor și mecanismelor necesare pentru protecția eficace a drepturilor fundamentale ale persoanelor vizate, în special pentru protecția vieții private și a datelor cu caracter personal ale acestora. Prezenta propunere include, de asemenea, dispoziții concepute special pentru a spori securitatea datelor cu caracter personal ale persoanelor fizice stocate în SIS.

Pentru ca sistemul să funcționeze, nu vor mai fi necesare alte procese sau armonizări la nivelul UE. Măsura avută în vedere este proporțională, deoarece acțiunea la nivelul UE întreprinsă pentru atingerea obiectivelor definite nu depășește ceea ce este necesar.

- **Alegerea instrumentului**

Revizuirea propusă va lua, de asemenea, forma unui regulament și va înlocui Regulamentul (CE) nr. 1987/2006. Această abordare a fost urmată, de asemenea, în ceea ce privește Decizia 2007/533/JAI a Consiliului și, dat fiind faptul că ambele instrumente sunt legate în mod intrinsec, trebuie aplicată și în legătură cu Regulamentul (CE) nr. 1987/2006. Decizia 2007/533/JAI a fost adoptată ca un așa-numit „instrument aferent celui de al treilea pilon” în temeiul vechiului Tratat privind Uniunea Europeană. Aceste instrumente aferente „celui de al treilea pilon” au fost adoptate de Consiliu fără Parlamentul European în calitate de colegiuitor. Temeiul juridic al prezentei propuneri îl constituie Tratatul privind funcționarea Uniunii Europene (TFUE), întrucât structura pe piloni a încetat să existe odată cu intrarea în vigoare a Tratatului de la Lisabona la 1 decembrie 2009. Temeiul juridic impune utilizarea procedurii legislative ordinare. Trebuie să se opteze pentru un regulament (al Parlamentului European și al Consiliului) deoarece dispozițiile urmează să fie obligatorii și să se aplice direct în toate statele membre.

Propunerea va avea la bază și va îmbunătăți un sistem centralizat existent prin intermediul căruia statele membre cooperează între ele, ceea ce necesită o arhitectură comună și norme de operare obligatorii comune. În plus, propunerea stabilește norme obligatorii privind accesul la sistem, inclusiv în scopul asigurării respectării legii, care sunt uniforme pentru toate statele membre, precum și pentru Agenția Europeană pentru Gestionarea Operațională a Sistemelor

Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție[15] (eu-LISA). Începând cu 9 mai 2013, eu-LISA este responsabilă cu gestionarea operațională a SIS central, care constă în toate sarcinile necesare pentru a asigura funcționarea deplină a SIS central, 24 de ore pe zi, 7 zile pe săptămână. Prezenta propunere se bazează pe responsabilitățile eu-LISA în ceea ce privește SIS.

În plus, propunerea prevede norme direct aplicabile care să permită accesul persoanelor vizate la datele care le privesc și la căi de atac, fără să fie nevoie de măsuri de punere în aplicare suplimentare în acest sens.

În consecință, nu se poate alege ca instrument legislativ decât un regulament.

3. REZULTATE ALE EVALUĂRILOR *EX POST*, CONSULTĂRILOR PĂRȚILOR INTERESATE ȘI EVALUĂRII IMPACTULUI

- **Evaluările *ex-post*/verificarea adecvării legislației existente**

În conformitate cu Regulamentul (CE) nr. 1987/2006 și cu Decizia 2007/533/JAI a Consiliului[16], la trei ani după intrarea sa în funcțiune, Comisia a efectuat o evaluare globală a sistemului SIS II central, precum și a schimbului bilateral și multilateral de informații suplimentare dintre statele membre.

Evaluarea a vizat în mod specific revizuirea aplicării articolului 24 din Regulamentul (CE) nr. 1987/2006 în scopul efectuării propunerilor necesare de modificare a dispozițiilor acestui articol pentru a se ajunge la un nivel mai ridicat de armonizare a criteriilor de introducere a semnalărilor.

Rezultatele evaluării au evidențiat necesitatea unor modificări ale temeiului juridic al SIS pentru a oferi un răspuns mai bun la noile provocări în materie de securitate și migrație. Printre acestea se numără, de exemplu, o propunere privind introducerea obligatorie în SIS a interdicțiilor de intrare pentru o mai bună asigurare a respectării acestora, consultarea obligatorie între statele membre în vederea evitării situațiilor în care o persoană face obiectul unei interdicții de intrare și deține totodată un permis de ședere, opțiunea de identificare și de localizare a persoanelor pe baza amprentelor lor digitale prin utilizarea unui nou sistem automat de identificare a amprentelor digitale și extinderea în sistem a elementelor biometrice de identificare.

Rezultatele evaluării au arătat, de asemenea, că este nevoie să se aducă modificări de ordin juridic pentru a îmbunătăți funcționarea tehnică a sistemului și pentru a raționaliza procesele naționale. Aceste măsuri vor spori eficiența și eficacitatea SIS prin facilitarea utilizării sale și prin reducerea sarcinilor inutile. Sunt concepute măsuri suplimentare pentru a îmbunătăți calitatea datelor și transparența sistemului printr-o descriere mai clară a sarcinilor de raportare specifice ale statelor membre și ale eu-LISA.

Rezultatele evaluării cuprinzătoare (raportul de evaluare și documentul de lucru conex au fost adoptate la 21 decembrie 2016[17]) au constituit baza măsurilor incluse în prezenta propunere.

---

15 Instituită prin Regulamentul (UE) nr. 1077/2011 al Parlamentului European și al Consiliului din 25 octombrie 2011 de instituire a Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (JO L 286, 1.11.2011, p. 1).

16 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).

17 Raportul către Parlamentul European și Consiliu privind evaluarea Sistemului de informații Schengen de a doua generație (SIS II) în conformitate cu articolul 24 alineatul (5), articolul 43 alineatul (3) și

În plus, în conformitate cu articolul 19 din Directiva 2008/115/CE privind returnarea, Comisia a publicat, în 2014, o comunicare privind politica UE în materie de returnare[18], care prezintă informații referitoare la aplicarea directivei menționate. Comunicarea a concluzionat că ar trebui consolidat și mai mult potențialul SIS în domeniul politicii de returnare, a menționat că revizuirea SIS II oferă ocazia de a îmbunătăți consecvența dintre politica de returnare și SIS II și a sugerat impunerea unei obligații a statelor membre de a introduce în SIS II semnalările privind refuzul intrării în cazul interdicțiilor de intrare emise în temeiul Directivei privind returnarea.

- **Consultările părților interesate**

În perioada de evaluare de către Comisie a SIS, părțile interesate relevante, inclusiv delegații din cadrul Comitetului SISVIS în temeiul procedurii stabilite la articolul 51 din Regulamentul (CE) nr. 1987/2006, au fost invitate să formuleze observații și sugestii. Din comitetul menționat fac parte reprezentanți ai statelor membre atât în ceea ce privește chestiunile operaționale privind SIRENE (cooperarea transfrontalieră în legătură cu SIS), cât și în ceea ce privește chestiunile tehnice în materie de dezvoltare și întreținere a SIS și a aplicației SIRENE conexe.

Delegații au răspuns la chestionare detaliate în cadrul procesului de evaluare. În cazul în care au fost necesare clarificări suplimentare sau subiectul a trebuit să fie dezvoltat mai mult, s-a recurs la schimburi de e-mailuri sau la interviuri specifice.

Acest proces iterativ a permis abordarea chestiunilor într-un mod cuprinzător și transparent. Pe parcursul anilor 2015 și 2016, delegații din cadrul Comitetului SISVIS au discutat aceste chestiuni cu ocazia unor reuniuni și ateliere specifice.

Comisia a consultat, de asemenea, în mod specific autoritățile naționale pentru protecția datelor din statele membre și membrii Grupului de coordonare a supravegherii SIS II în domeniul protecției datelor. Răspunzând la un chestionar specific, statele membre și-au împărtășit experiențele în ceea ce privește cererile de acces ale persoanelor vizate și activitatea autorităților naționale pentru protecția datelor. Răspunsurile la chestionarul din iunie 2015 au fost luate în considerare la elaborarea prezentei propuneri.

Pe plan intern, Comisia a înființat un grup de coordonare între servicii, din care au făcut parte Secretariatul General, Direcția Generală Migrație și Afaceri Interne, Direcția Generală Justiție și Consumatori, Direcția Generală Resurse Umane și Securitate și Direcția Generală Informatică. Acest grup de coordonare a monitorizat procesul de evaluare și a oferit îndrumările necesare, după caz.

La formularea constatărilor evaluării s-au luat, de asemenea, în considerare probele colectate în timpul vizitelor de evaluare la fața locului în statele membre, analizând în detaliu modul în care SIS este utilizat în practică. În acest cadru au avut loc discuții și interviuri cu practicieni, cu personalul birourilor SIRENE și cu autoritățile naționale competente.

De asemenea, în cadrul Grupului de contact al Comisiei pentru Directiva privind returnarea, cu ocazia reuniunilor sale din 16 noiembrie 2015, 18 martie 2016 și 20 iunie 2016, autoritățile competente în materie de returnare din statele membre au fost invitate să prezinte observații și

articolul 50 alineatul (5) din Regulamentul (CE) nr. 1987/2006 și cu articolul 59 alineatul (3) și articolul 66 alineatul (5) din Decizia 2007/533/JAI și documentul de lucru însoțitor.

[18] COM(2014) 199 final.

sugestii, în special cu privire la consecințele unei eventuale obligații de a introduce în SIS semnalări pentru toate interdicțiile de intrare emise în conformitate cu Directiva 2008/115/CE.

În lumina acestor observații, propunerea prevede măsuri de îmbunătățire a eficienței și a eficacității sistemului din punct de vedere tehnic și operațional.

- **Obținerea și utilizarea expertizei**

Pe lângă consultările cu părțile interesate, Comisia a solicitat, de asemenea, expertiză externă, comandând patru studii, ale căror constatări au fost utilizate la elaborarea prezentei propuneri:

- Evaluarea tehnică a SIS (*SIS Technical Assessment*) (Kurt Salmon)[19]

Această evaluare a identificat principalele probleme ale funcționării SIS și nevoile viitoare care ar trebui satisfăcute, principalele aspecte vizate fiind maximizarea asigurării continuității activității și garantarea faptului că arhitectura globală se poate adapta la creșterea cerințelor de capacitate.

- Evaluarea impactului în materie de TIC al posibilelor îmbunătățiri ale arhitecturii SIS II (*ICT Impact Assessment of Possible Improvements to the SIS II Architecture*) (Kurt Salmon)[20]

Acest studiu a evaluat costul actual al funcționării SIS la nivel național și a analizat două scenarii tehnice posibile de îmbunătățire a sistemului. Ambele scenarii includ o serie de propuneri tehnice axate pe îmbunătățirea sistemului central și a arhitecturii globale.

- Evaluarea impactului în materie de TIC al îmbunătățirilor tehnice ale arhitecturii SIS II - Raport final (*ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report*), 10 noiembrie 2016 (Wavestone)[21]

Acest studiu a evaluat impacturile asupra statelor membre din punctul de vedere al costurilor aferente realizării unei copii naționale prin analizarea a trei scenarii (un sistem complet centralizat, realizarea unor N.SIS standardizate, dezvoltate și furnizate de eu-LISA statelor membre, și realizarea unor N.SIS distincte, cu standarde tehnice comune).

- Studiu privind fezabilitatea și implicațiile creării în cadrul Sistemului de informații Schengen a unui sistem la nivelul UE pentru schimbul de date privind deciziile de returnare și pentru monitorizarea respectării acestor decizii *(Study on the feasibility and implications of setting up within the framework of the Schengen Information System an EU-wide system for exchanging data on and monitoring compliance with return decisions)* (PwC)[22]

---

19 Comisia Europeană, RAPORT FINAL - Evaluarea tehnică a SIS II (*FINAL REPORT - SIS II technical assessment*).

20 Comisia Europeană, RAPORT FINAL - Evaluarea impactului în materie de TIC al posibilelor îmbunătățiri ale arhitecturii SIS II (*ICT Impact Assessment of Possible Improvements to the SIS II Architecture*), 2016.

21 Comisia Europeană, RAPORT FINAL - Evaluarea impactului în materie de TIC al îmbunătățirilor tehnice ale arhitecturii SIS II - Raport final (*FINAL REPORT — ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report*), 10 noiembrie 2016 (Wavestone).

22 Studiu privind fezabilitatea și implicațiile creării în cadrul SIS a unui sistem la nivelul UE pentru schimbul de date privind deciziile de returnare și pentru monitorizarea respectării acestor decizii (*Study*

Acest studiu evaluează fezabilitatea și implicațiile tehnice și operaționale ale modificărilor propuse care vizează ca SIS să fie utilizat în mai mare măsură pentru returnarea migranților în situație neregulamentară și pentru a împiedica reintrarea lor.

- **Evaluarea impactului**

Comisia nu a efectuat o evaluare a impactului.

Cele trei evaluări independente menționate mai sus au stat la baza analizei din punct de vedere tehnic a impacturilor modificărilor propuse a fi aduse sistemului. În plus, Comisia a efectuat două revizuiri ale Manualului SIRENE din 2013, și anume de la intrarea în funcțiune a SIS II la 9 aprilie 2013 și de când Decizia 2007/533/JAI a devenit aplicabilă. Această activitate a inclus o evaluare la jumătatea perioadei, care a condus la lansarea unui nou Manual SIRENE[23] la 29 ianuarie 2015. Comisia a adoptat, de asemenea, un catalog de bune practici și recomandări[24]. În plus, eu-LISA și statele membre aduc sistemului îmbunătățiri tehnice periodice, iterative. S-a considerat că în prezent aceste opțiuni au fost epuizate, fiind necesară o modificare mai amplă a temeiului juridic. Claritatea în domenii cum ar fi aplicarea sistemelor utilizatorilor finali, precum și normele detaliate privind ștergerea unei semnalări nu poate fi obținută doar prin îmbunătățirea punerii în aplicare și a asigurării respectării reglementărilor.

De asemenea, Comisia a efectuat o evaluare cuprinzătoare a SIS, în conformitate cu articolul 24 alineatul (5), articolul 43 alineatul (3) și articolul 50 alineatul (5) din Regulamentul (CE) nr. 1987/2006 și cu articolul 59 alineatul (3) și articolul 66 alineatul (5) din Decizia 2007/533/JAI, și a publicat un document de lucru însoțitor. Rezultatele evaluării cuprinzătoare (raportul de evaluare și documentul de lucru conex au fost adoptate la 21 decembrie 2016) au constituit baza măsurilor incluse în prezenta propunere.

Mecanismul de evaluare Schengen, prevăzut în Regulamentul (UE) nr. 1053/2013[25], permite evaluarea juridică și operațională periodică a funcționării SIS în statele membre. Evaluările sunt efectuate în comun de către Comisie și statele membre. Prin intermediul acestui mecanism, Consiliul face recomandări statelor membre, pe baza evaluărilor realizate în cadrul programului multianual și a celui anual. Ca urmare a naturii lor individuale, aceste recomandări nu pot înlocui norme obligatorii din punct de vedere juridic care sunt aplicabile în același timp pentru toate statele membre care utilizează SIS.

Comitetul SISVIS discută periodic chestiuni tehnice și operaționale de ordin practic. Deși aceste întâlniri sunt esențiale pentru cooperarea dintre Comisie și statele membre, rezultatul

---

on the feasibility and implications of setting up within the framework of the SIS and EU-wide system for exchanging data on and monitoring compliance with return decisions), 4 aprilie 2015, PwC.

[23] Decizia de punere în aplicare (UE) 2015/219 a Comisiei din 29 ianuarie 2015 de înlocuire a anexei la Decizia de punere în aplicare 2013/115/UE privind Manualul SIRENE și alte măsuri de punere în aplicare a Sistemului de Informații Schengen de a doua generație (SIS II) (JO L 44, 18.2.2015, p. 75).

[24] Recomandarea Comisiei de instituire a unui catalog de recomandări și bune practici pentru aplicarea corectă a Sistemului de informații Schengen de a doua generație (SIS II) și efectuarea schimbului de informații suplimentare de către autoritățile competente ale statelor membre care pun în aplicare și utilizează SIS II [C(2015)9169/1].

[25] Regulamentul (UE) nr. 1053/2013 din 7 octombrie 2013 de instituire a unui mecanism de evaluare și monitorizare în vederea verificării aplicării acquis-ului Schengen și de abrogare a Deciziei Comitetului executiv din 16 septembrie 1998 de instituire a Comitetului permanent pentru evaluarea și punerea în aplicare a Acordului Schengen (JO L 295, 6.11.2013, p. 27).

discuțiilor (în lipsa unor modificări legislative) nu poate soluționa problemele apărute din cauza practicilor naționale divergente, de exemplu.

Modificările propuse în prezentul regulament nu au o importanță economică semnificativă sau un impact semnificativ asupra mediului. Totuși, se preconizează că aceste modificări vor avea un impact social pozitiv semnificativ, deoarece oferă o securitate sporită, permițând o mai bună identificare a persoanelor care utilizează identități false, a infractorilor a căror identitate rămâne necunoscută după comiterea unei infracțiuni grave, precum și a migranților în situație neregulamentară care profită de spațiul fără controale la frontierele interne. Impactul acestor modificări asupra drepturilor fundamentale și a protecției datelor a fost analizat și este prezentat mai detaliat în secțiunea următoare („Drepturi fundamentale”).

La elaborarea propunerii s-au utilizat probele substanțiale colectate pentru a sta la baza evaluării globale a SIS de a doua generație, care a analizat funcționarea sistemului și domeniile în care se pot aduce îmbunătățiri. În plus, s-a efectuat un studiu de evaluare a impactului din punctul de vedere al costurilor pentru a se asigura faptul că arhitectura națională aleasă era cea mai adecvată și proporțională.

- **Drepturile fundamentale și protecția datelor**

Prezenta propunere dezvoltă și îmbunătățește un sistem existent, mai degrabă decât să înființeze unul nou, și, prin urmare, se bazează pe garanții importante și eficace care au fost deja instituite. Cu toate acestea, deoarece sistemul continuă să prelucreze date cu caracter personal și va prelucra categorii suplimentare de date biometrice sensibile, există impacturi potențiale asupra drepturilor fundamentale ale persoanelor. Aceste elemente au fost analizate în detaliu și s-au instituit garanții suplimentare pentru a limita colectarea și prelucrarea ulterioară a datelor la ceea ce este strict necesar și obligatoriu din punct de vedere operațional și pentru a restricționa accesul la datele respective la persoanele care au o nevoie operațională de a le prelucra. În prezenta propunere s-au stabilit termene clare în materie de păstrare a datelor, se recunosc explicit și există dispoziții privind drepturile persoanelor de accesare și rectificare a datelor care le privesc și de a solicita ștergerea acestora în conformitate cu drepturile lor fundamentale (a se vedea secțiunea referitoare la protecția datelor și securitate).

În plus, propunerea întărește măsurile de protecție a drepturilor fundamentale, deoarece stabilește în legislație cerințele privind ștergerea unei semnalări și introduce o evaluare a proporționalității în cazul prelungirii valabilității unei semnalări. Propunerea definește garanții extinse și solide privind utilizarea elementelor biometrice de identificare pentru a se evita prejudicierea unor persoane nevinovate.

Propunerea prevede, de asemenea, securitatea sistemului de la un capăt la altul, ceea ce asigură o protecție sporită pentru datele stocate în acesta. Prin introducerea unei proceduri clare de gestionare a incidentelor, precum și prin îmbunătățirea asigurării continuității activității în ceea ce privește SIS, prezenta propunere respectă pe deplin Carta drepturilor fundamentale a Uniunii Europene[26], nu numai referitor la dreptul la protecția datelor cu caracter personal. Dezvoltarea și menținerea eficacității SIS va contribui la asigurarea securității persoanelor în societate.

Propunerea prevede modificări semnificative în ceea ce privește elementele biometrice de identificare. În plus față de amprentele digitale, amprentele palmare ar trebui, de asemenea, să fie colectate și stocate, dacă sunt îndeplinite cerințele legale. Fișierele amprentelor digitale

[26] Carta drepturilor fundamentale a Uniunii Europene (2012/C 326/02).

sunt atașate la semnalările alfanumerice din SIS, astfel cum se prevede la articolul 24. În viitor, ar trebui să fie posibil să se efectueze căutări în aceste date dactiloscopice (amprente digitale și amprente palmare) cu ajutorul amprentelor digitale găsite la locul unei infracțiuni, cu condiția ca infracțiunea să constituie o infracțiune gravă sau o infracțiune de terorism și să fie posibil să se afirme cu un grad ridicat de probabilitate că aparțin autorului. În caz de incertitudine în ceea ce privește identitatea unei persoane pe baza documentelor sale, autoritățile competente ar trebui să verifice amprentele digitale prin efectuarea de căutări în baza de date din SIS.

Propunerea prevede colectarea și stocarea de date suplimentare (cum ar fi detaliile documentelor de identificare personale) care să faciliteze activitatea agenților de pe teren pentru a stabili identitatea unei persoane.

Propunerea garantează dreptul persoanei vizate la căi de atac eficiente, disponibile pentru a contesta orice decizie, care includ, în orice caz, o cale de atac eficientă în fața unei instanțe judecătorești în conformitate cu articolul 47 din Carta drepturilor fundamentale.

4. IMPLICAȚII BUGETARE

SIS constituie un sistem de informații unic. În consecință, cheltuielile prevăzute în două propuneri [prezenta propunere și Propunerea de regulament privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală] nu ar trebui considerate ca fiind două cuantumuri distincte, ci ca unul singur. Implicațiile bugetare ale modificărilor necesare pentru punerea în aplicare a ambelor propuneri sunt incluse într-o singură fișă financiară legislativă.

Datorită naturii complementare a celei de a treia propuneri (privind returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală), implicațiile bugetare sunt abordate separat și într-o fișa financiară distinctă care vizează doar instituirea acestei categorii specifice de semnalări.

Pe baza unei evaluări a diverselor aspecte ale activității necesare în ceea ce privește rețeaua, și anume SIS central de care este responsabilă eu-LISA și dezvoltările naționale din statele membre, cele două propuneri de regulamente vor necesita o sumă globală de 64,3 milioane EUR pentru perioada 2018-2020.

Această sumă include o creștere a lărgimii de bandă a TESTA-NG ca urmare a faptului că, în conformitate cu cele două propuneri, rețeaua va transmite fișiere cu amprente digitale și imagini faciale care necesită o rată de transfer mai ridicată și o capacitate sporită (9,9 milioane EUR). Această sumă acoperă, de asemenea, costurile aferente cheltuielilor cu personalul și cheltuielilor operaționale (17,6 milioane EUR). eu-LISA a informat Comisia că în ianuarie 2018 este planificată recrutarea a 3 noi agenți contractuali pentru a începe faza de dezvoltare în timp util, astfel încât funcționalitățile actualizate ale SIS să devină operaționale în 2020. Prezenta propunere implică modificări tehnice ale SIS central pentru extinderea anumitor categorii de semnalări existente și furnizarea unor noi funcționalități. Fișa financiară atașată la prezenta propunere reflectă aceste modificări.

În plus, Comisia a efectuat un studiu de evaluare a impactului din punctul de vedere al costurilor pentru a estima cheltuielile aferente dezvoltărilor naționale care trebuie efectuate în

temeiul prezentei propuneri[27]. Costul estimat este de 36,8 milioane EUR și ar trebui să fie acoperit prin alocarea unei sume forfetare statelor membre. Astfel, fiecare stat membru va primi suma de 1,2 milioane EUR pentru actualizarea sistemului său național în conformitate cu cerințele stabilite în prezenta propunere, inclusiv pentru crearea unei copii naționale parțiale, dacă aceasta nu există deja, sau a unui un sistem de rezervă.

Se preconizează o reprogramare a restului pachetului financiar destinat frontierelor inteligente din cadrul Fondului pentru securitate internă în vederea efectuării actualizărilor și a realizării funcționalităților prevăzute în cele două propuneri. Regulamentul de instituire în cadrul FSI a sprijinului pentru frontiere[28] este instrumentul financiar în care a fost inclus bugetul alocat punerii în aplicare a pachetului privind frontierele inteligente. Articolul 5 din regulamentul menționat prevede că un buget de 791 de milioane EUR va fi executat printr-un program pentru dezvoltarea de sisteme informatice în vederea gestionării fluxurilor migratorii la frontierele externe, în condițiile prevăzute la articolul 15. Din cele 791 de milioane EUR menționate mai sus, 480 de milioane EUR sunt rezervate pentru dezvoltarea sistemului de intrare-ieșire și 210 milioane EUR pentru dezvoltarea sistemului european de informații și de autorizare privind călătoriile (ETIAS). Suma rămasă va fi utilizată parțial pentru a acoperi costurile aferente modificărilor prevăzute în cele două propuneri privind SIS.

5. ELEMENTE DIVERSE

- **Planurile de implementare și mecanismele de monitorizare, evaluare și raportare**

Comisia, statele membre și eu-LISA vor reexamina și monitoriza în mod regulat utilizarea SIS, pentru a se asigura că acesta continuă să funcționeze în mod eficace și eficient. Comisia va fi asistată de Comitetul SISVIS pentru a pune în aplicare măsurile tehnice și operaționale descrise în propunere.

În plus, la articolul 54 alineatele (7) și (8), prezenta propunere de regulament include dispoziții privind un proces de revizuire și evaluare formal și regulat.

Din doi în doi ani, eu-LISA trebuie să prezinte un raport Parlamentului European și Consiliului privind funcționarea tehnică - inclusiv securitatea - SIS, infrastructura de comunicare ce stă la baza acestuia și schimbul bilateral și multilateral de informații suplimentare dintre statele membre.

În plus, din patru în patru ani, Comisia trebuie să efectueze o evaluare globală a SIS și a schimbului de informații dintre statele membre, pe care să o transmită Parlamentului și Consiliului. Aceasta va:

- examina rezultatele obținute în raport cu obiectivele;
- evalua dacă raționamentul care stă la baza sistemului rămâne valabil;
- examina modul în care regulamentul este aplicat în cazul sistemului central;

[27] Wavestone, „Evaluarea impactului în materie de TIC al îmbunătățirilor tehnice ale arhitecturii SIS II - Raport final” (*ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report*), 10 noiembrie 2016, scenariul 3 - realizarea unor N.SIS II distincte.

[28] 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 (JO L 150, 20.5.2014, p. 143).

- evalua securitatea sistemului central;
- analiza implicațiile pentru funcționarea în viitor a sistemului.

De acum, eu-LISA este, de asemenea, însărcinată să furnizeze statistici zilnice, lunare și anuale privind utilizarea SIS și să asigure monitorizarea continuă a sistemului și a funcționării sale în raport cu obiectivele.

- **Explicații detaliate cu privire la noile dispoziții ale propunerii**

Dispoziții care sunt comune prezentei propuneri și Propunerii de regulament privind instituirea, funcționarea și utilizarea SIS în domeniul cooperării polițienești și al cooperării judiciare în materie penală:

- dispozițiile generale (articolele 1-3);
- arhitectura tehnică a SIS și modul de funcționare a acestuia (articolele 4-14);
- responsabilitățile eu-LISA (articolele 15-18);
- dreptul de acces la semnalări și păstrarea acestora (articolele 29, 30, 31, 33 și 34);
- normele generale de prelucrare a datelor și de protecție a datelor (articolele 36-53);
- monitorizare și statistici (articolul 54).

Utilizarea SIS de la un capăt la altul

Cu peste 2 milioane de utilizatori finali în cadrul autorităților competente din întreaga Europă, SIS este un instrument de schimb de informații utilizat pe o scară foarte largă și extrem de eficace. Aceste propuneri includ norme care reglementează funcționarea completă a sistemului de la un capăt la altul, inclusiv a SIS central gestionat de eu-LISA, a sistemelor naționale și a aplicațiilor destinate utilizatorilor finali. Aceste propuneri abordează nu numai sistemul central și sistemele naționale, ci și nevoile tehnice și operaționale ale utilizatorilor finali.

Articolul 9 alineatul (2) precizează faptul că utilizatorii finali trebuie să primească datele necesare pentru îndeplinirea sarcinilor care le revin (în special, toate datele necesare pentru identificarea persoanei vizate și pentru întreprinderea acțiunii necesare). De asemenea, prevede un plan de acțiune comun pentru punerea în aplicare a SIS de către statele membre, asigurând armonizarea între toate sistemele naționale. Articolul 6 prevede că fiecare stat membru trebuie să asigure disponibilitatea neîntreruptă a datelor din SIS pentru utilizatorii finali, în vederea maximizării beneficiilor operaționale prin reducerea riscului de indisponibilitate.

Articolul 10 alineatul (3) asigură faptul că securitatea prelucrării datelor include, de asemenea, activitățile de prelucrare a datelor efectuate de utilizatorii finali. Articolul 14 impune statelor membre obligația de a se asigura că personalul care are acces la SIS beneficiază de formare regulată și continuă cu privire la securitatea datelor și la normele de protecție a datelor.

Ca urmare a includerii acestor măsuri, prezenta propunere reglementează într-un mod mai cuprinzător întreaga funcționare a SIS, de la un capăt la altul, stabilind norme și obligații pentru milioanele de utilizatori finali din întreaga Europă. Pentru a utiliza SIS la nivelul său maxim de eficacitate, statele membre ar trebui să se asigure că de fiecare dată când utilizatorii

lor finali au dreptul de a efectua o căutare într-o bază de date națională a poliției sau în materie de imigrație, aceştia efectuează, de asemenea, în paralel căutări în SIS. În acest mod SIS își poate îndeplini obiectivul ca principală măsură compensatorie în spațiul fără controale la frontierele interne și statele membre pot aborda mai bine dimensiunea transfrontalieră a criminalității și mobilitatea infractorilor. Această căutare paralelă trebuie să rămână conformă cu articolul 4 din Directiva (UE) 2016/680[29].

Asigurarea continuității activității

Propunerile consolidează dispozițiile referitoare la asigurarea continuității activității, atât la nivel național, cât și în ceea ce privește eu-LISA (articolele 4, 6, 7 și 15). Acestea asigură faptul că SIS va continua să rămână funcțional și accesibil pentru personalul de pe teren, chiar dacă există probleme care afectează sistemul.

Calitatea datelor

Propunerea menține principiul conform căruia statul membru care este proprietarul datelor răspunde, de asemenea, de exactitatea datelor introduse în SIS (articolul 39). Cu toate acestea, este necesar să se prevadă un mecanism central gestionat de eu-LISA care să permită statelor membre să reexamineze periodic semnalările în care câmpurile de date obligatorii pot ridica probleme de calitate. Prin urmare, articolul 15 din propunere împuternicește eu-LISA să furnizeze statelor membre, la intervale regulate, rapoarte privind calitatea datelor. Această activitate poate fi facilitată de instituirea unui registru de date pentru elaborarea de rapoarte statistice și privind calitatea datelor (articolul 54). Aceste îmbunătățiri reflectă concluziile provizorii ale Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate.

Fotografii, imagini faciale, date dactiloscopice și profiluri ADN

Posibilitatea de a efectua căutări cu ajutorul amprentelor digitale pentru a identifica o persoană este deja prevăzută la articolul 22 din Regulamentul (CE) nr. 1987/2006 și din Decizia 2007/533/JAI a Consiliului. Propunerile introduc obligația de a efectua această căutare dacă identitatea persoanei nu poate fi stabilită în niciun alt mod. În prezent, imaginile faciale se pot utiliza doar pentru a confirma identitatea unei persoane ca urmare a unei căutări alfanumerice, mai degrabă decât ca bază pentru efectuarea unei căutări. În plus, modificările aduse articolelor 22 și 28 prevăd utilizarea imaginilor faciale, a fotografiilor și a amprentelor palmare pentru efectuarea de căutări în sistem și pentru identificarea persoanelor, atunci când acest lucru va fi posibil din punct de vedere tehnic. Dactiloscopia este studierea științifică a amprentelor digitale ca metodă de identificare. Experții în dactiloscopie recunosc faptul că amprentele palmare se caracterizează prin unicitate și că acestea conțin puncte de referință care permit comparații fiabile și concludente, la fel ca și amprentele digitale. Amprentele palmare se pot utiliza pentru stabilirea identității unei persoane în același mod ca și amprentele digitale. Prelevarea amprentelor palmare odată cu cele zece amprente digitale obținute prin apăsarea degetului de la un capăt al unghiei la celălalt și cu cele zece amprente digitale plane constituie o practică a poliției de mai multe decenii. Amprentele palmare sunt utilizate în principal în scopul identificării, atunci când persoana vizată și-a deteriorat în mod

[29] 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 (JO L 119, 4.5.2016, p. 89).

intenționat sau neintenționat vârfurile degetelor. Această deteriorare poate fi rezultatul unei încercări de a evita identificarea sau prelevarea amprentelor digitale sau rezultatul unui accident ori al lucrului manual susținut. În cadrul discuțiilor privind normele tehnice ale sistemului automat de identificare a amprentelor digitale (AFIS) din SIS, statele membre au declarat că au reușit astfel să identifice migranții în situație neregulamentară care și-au deteriorat în mod intenționat vârfurile degetelor, încercând în acest mod să evite identificarea. Prelevarea amprentelor palmare de către autoritățile statelor membre a permis identificarea ulterioară.

Utilizarea imaginilor faciale pentru identificare va asigura o coerență sporită între SIS și sistemul propus al UE de intrare/ieșire, porțile electronice și chioșcurile de control self-service. Această funcționalitate se va utiliza exclusiv la punctele obișnuite de trecere a frontierei.

Accesul autorităților la SIS - utilizatorii instituționali

Prezenta subsecțiune este menită să descrie noile elemente ale drepturilor de acces în ceea ce privește agențiile UE (utilizatorii instituționali). Drepturile de acces ale autorităților naționale competente nu au fost modificate.

Europol (articolul 30) și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă - precum și echipele sale, echipele de personal implicat în sarcini legate de returnare și membrii echipelor de sprijin pentru gestionarea migrației - și unitatea centrală a ETIAS din cadrul agenției (articolele 31 și 32) au acces la SIS și la datele din SIS de care au nevoie. Sunt instituite garanții corespunzătoare în vederea asigurării faptului că datele din sistem sunt protejate în mod adecvat (inclusiv articolul 33, care prevede că aceste organisme pot accesa doar datele care le sunt necesare în scopul îndeplinirii sarcinilor care le revin).

Aceste modificări extind accesul Europol la SIS la semnalările privind refuzul intrării, ceea ce asigură faptul că acesta poate utiliza în mod optim sistemul pentru a-și îndeplini atribuțiile care îi revin, și adăugă noi dispoziții menite să garanteze că Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă, precum și echipele sale pot avea acces la sistem în timpul diferitelor operațiuni efectuate în limitele mandatului lor de a acorda asistență statelor membre. De asemenea, în temeiul Propunerii Comisiei de regulament al Parlamentului European și al Consiliului de instituire a unui sistem european de informații și de autorizare privind călătoriile (ETIAS)[30], unitatea centrală a ETIAS din cadrul Agenției Europene pentru Poliția de Frontieră și Garda de Coastă va verifica în SIS, prin intermediul ETIAS, dacă un resortisant al unei țări terțe care solicită o autorizație de călătorie face obiectul unei semnalări în SIS. În acest scop, unitatea centrală a ETIAS va avea, de asemenea, acces la SIS[31].

Articolul 29 alineatul (3) stabilește că autoritățile naționale responsabile în domeniul vizelor pot, de asemenea, în îndeplinirea sarcinilor care le revin să acceseze semnalările privind documente emise în conformitate cu Regulamentul 2008/.... privind instituirea, funcționarea și utilizarea SIS în domeniul cooperării polițienești și al cooperării judiciare în materie penală.

Acest lucru va permite organismelor respective să aibă acces la SIS și la datele din SIS care le sunt necesare pentru a-și îndeplini sarcinile, instituindu-se totodată garanții corespunzătoare

30 COM (2016)731 final.

31 Unității centrale a ETIAS i se acordă acces la datele introduse în conformitate cu articolele 24 și 27 din prezentul regulament.

pentru a se asigura faptul că datele din sistem sunt protejate în mod adecvat (inclusiv articolul 35 care prevede că aceste organisme pot accesa doar datele care le sunt necesare în scopul îndeplinirii sarcinilor care le revin).

Refuzul intrării și al șederii

În prezent, în conformitate cu articolul 24 alineatul (3) din Regulamentul SIS II, un stat membru poate introduce în SIS o semnalare privind persoanele care fac obiectul unei interdicții de intrare emise în temeiul nerespectării legislației naționale în materie de migrație. Articolul 24 alineatul (3) revizuit prevede obligația de a introduce în SIS o semnalare în orice caz în care pentru un resortisant al unei țări terțe aflat în situație de ședere ilegală s-a emis o interdicție de intrare în conformitate cu dispoziții care respectă Directiva 2008/115/CE. De asemenea, acesta stabilește termenele și condițiile de introducere a unor astfel de semnalări după ce resortisantul țării terțe a părăsit teritoriile statelor membre ca urmare a respectării unei obligații de returnare. Această dispoziție este introdusă pentru a se evita ca interdicțiile de intrare să fie vizibile în SIS, în timp ce resortisantul țării terțe în cauză este încă prezent pe teritoriul UE. Dat fiind faptul că interdicțiile de intrare nu permit reintrarea pe teritoriile statelor membre, acestea pot intra în vigoare numai după returnarea resortisanților țărilor terțe în cauză. În același timp, statele membre ar trebui să ia toate măsurile necesare pentru a se asigura că nu există un decalaj temporar între momentul returnării și activarea în SIS a semnalării privind refuzul intrării și al șederii.

Prezenta propunere este strâns legată de propunerea Comisiei[32] referitoare la utilizarea SIS pentru returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală, care stabilește condițiile și procedurile de introducere în SIS a semnalărilor privind deciziile de returnare. Propunerea menționată include un mecanism pentru a monitoriza dacă resortisanții țărilor terțe care fac obiectul unei decizii de returnare părăsesc efectiv teritoriul UE și un mecanism de avertizare în caz de nerespectare a acestei decizii. Articolul 26 stabilește procesul de consultare pe care statele membre trebuie să îl urmeze atunci când identifică semnalări privind refuzul intrării și al șederii - sau când doresc să introducă aceste semnalări - care intră în conflict cu alte decizii ale statelor membre, cum ar fi, de exemplu, un permis de ședere valabil. Aceste norme ar trebui să prevină apariția unor instrucțiuni contradictorii sau să soluționeze instrucțiunile contradictorii pe care aceste situații le pot crea, oferind, în același timp, orientări clare utilizatorilor finali cu privire la acțiunile care trebuie întreprinse în astfel de situații și autorităților statelor membre cu privire la oportunitatea ștergerii unei semnalări.

Articolul 27 [fostul articolul 26 din Regulamentul (CE) nr. 1987/2006] este menit să pună în aplicare regimul de sancțiuni al UE aplicabil resortisanților țărilor terțe care fac obiectul unei restricții de admitere pe teritoriul UE în conformitate cu articolul 29 din Tratatul privind Uniunea Europeană. Pentru a autoriza introducerea acestor semnalări era necesar să se prevadă obligativitatea datelor minime necesare în vederea identificării persoanei, și anume numele și data nașterii. Eliminarea de către Regulamentul (CE) nr. 1987/2006 a cerinței de a se introduce data nașterii a generat probleme semnificative, deoarece în SIS nu se poate crea o semnalare fără o dată de naștere, în conformitate cu normele tehnice ale sistemului și cu parametrii de căutare ai acestuia. Întrucât articolul 27 este indispensabil pentru a avea un regim de sancțiuni al UE care să fie eficient, în această privință nu se aplică cerința de proporționalitate.

[32] COM (2016)…

Pentru a se asigura o coerență sporită cu Directiva 2008/115/CE, terminologia utilizată atunci când se face referire la scopul semnalării („refuzul intrării și al ședерii”) a fost aliniată la formularea utilizată în directivă.

Diferențierea persoanelor care prezintă caracteristici similare

Pentru a se asigura faptul că datele sunt prelucrate și stocate în mod corespunzător și pentru a reduce riscul duplicării și al identificării eronate, articolul 41 stabilește procedura care trebuie urmată în cazul în care se constată, la introducerea unei noi semnalări, că în SIS există deja o intrare care prezintă caracteristici similare.

Protecția și securitatea datelor

Prezenta propunere aduce clarificări cu privire la responsabilitatea pentru prevenirea, raportarea și răspunsul la incidente care ar putea afecta securitatea sau integritatea infrastructurii SIS, a datelor din SIS sau a informațiilor suplimentare (articolele 10, 16 și 40).

Articolul 12 conține dispoziții privind păstrarea înregistrărilor care conțin istoricul semnalărilor și efectuarea de căutări în aceste înregistrări.

Articolul 15 alineatul (3) menține dispozițiile articolului 15 alineatul (3) din Regulamentul (CE) nr. 1987/2006 și prevede că Comisia rămâne responsabilă cu gestionarea contractelor aferente infrastructurii de comunicare, inclusiv cu sarcinile referitoare la execuția bugetară, la achiziții și la reînnoire. Aceste sarcini vor fi transferate către eu-LISA în a doua serie de propuneri privind SIS, în iunie 2017.

Articolul 21 extinde cerința ca statele membre să țină seama de proporționalitate înainte de a emite semnalări, aceasta aplicându-se, de asemenea, deciziilor prin care se stabilește dacă perioada de valabilitate a unei semnalări ar trebui să fie prelungită. Ca element de noutate însă, articolul 24 alineatul (2) litera (c) prevede obligația statelor membre de a crea în toate circumstanțele o semnalare privind persoanele a căror activitate intră sub incidența articolelor 1, 2, 3 și 4 din Decizia-cadru 2002/475/JAI a Consiliului privind combaterea terorismului.

Categoriile de date și prelucrarea datelor

Pentru a oferi informații mai ample și mai precise utilizatorilor finali în vederea facilitării și a accelerării întreprinderii acțiunii necesare, precum și pentru a permite o mai bună identificare a persoanei care face obiectul semnalării, prezenta propunere extinde tipurile de informații (articolul 20) care pot fi deținute despre persoanele în privința cărora s-a emis o semnalare, astfel încât printre aceste informații să se numere și următoarele elemente:

- dacă persoana este implicată în orice activitate care intră sub incidența articolelor 1, 2, 3 și 4 din Decizia-cadru 2002/475/JAI a Consiliului;
- dacă semnalarea se referă la un cetățean al UE sau la o altă persoană care beneficiază de drepturi de liberă circulație echivalente cu cele ale cetățenilor UE;
- dacă o decizie privind refuzul intrării se bazează pe dispozițiile de la articolul 24 sau de la articolul 27;
- tipul de infracțiune [pentru semnalările emise în temeiul articolului 24 alineatul (2)];

- detalii privind documentul de identitate sau de călătorie al persoanei vizate;
- o copie color a documentului de identitate sau de călătorie al persoanei vizate;
- fotografii și imagini faciale;
- amprente digitale și amprente palmare.

Deținerea datelor corespunzătoare este esențială pentru a se asigura identificarea exactă a unei persoane care este verificată la trecerea frontierei, care face obiectul unei verificări interne sau care solicită un permis de ședere. O identificare inexactă poate genera probleme legate de drepturile fundamentale; de asemenea, aceasta poate conduce la o situație în care nu pot fi luate măsuri subsecvente corespunzătoare, deoarece nu se știe că există o semnalare sau nu se cunoaște conținutul unei semnalări.

În ceea ce privește informațiile privind decizia care stă la baza unei semnalări, se pot distinge patru motive: o condamnare anterioară, astfel cum se menționează la articolul 24 alineatul (2) litera (a), o amenințare gravă la adresa securității, astfel cum se menționează la articolul 24 alineatul (2) litera (b), o interdicție de intrare, astfel cum se menționează la articolul 24 alineatul (3) și o măsură restrictivă, astfel cum se menționează la articolul 27. În vederea asigurării faptului că se întreprind acțiunile corespunzătoare în cazul obținerii unui rezultat pozitiv este, de asemenea, necesar să se indice dacă semnalarea se referă la un cetățean al UE sau la o altă persoană care beneficiază de drepturi de liberă circulație echivalente cu cele ale cetățenilor UE. Deținerea datelor corespunzătoare este esențială pentru a se asigura identificarea exactă a unei persoane care este verificată la trecerea frontierei, care face obiectul unei verificări interne sau care solicită un permis de ședere. O identificare inexactă poate genera probleme legate de drepturile fundamentale; de asemenea, aceasta poate conduce la o situație în care nu pot fi luate măsuri subsecvente corespunzătoare, deoarece nu se știe că există o semnalare sau nu se cunoaște conținutul unei semnalări.

De asemenea, prezenta propunere (la articolul 42) extinde lista datelor cu caracter personal care pot fi introduse și prelucrate în SIS în scopul tratării cazurilor de uzurpare de identitate, deoarece deținerea mai multor date facilitează identificarea victimei și a autorului uzurpării de identitate. Extinderea dispoziției în cauză nu implică niciun risc, deoarece toate aceste date nu pot fi introduse decât cu acordul victimei uzurpării de identitate. Acum vor fi incluse, de asemenea, următoarele:

- imagini faciale;
- amprente palmare;
- detalii privind documentele de identitate;
- adresa victimei;
- numele tatălui și al mamei victimei.

Articolul 20 prevede introducerea unor informații mai detaliate în semnalări, Printre acestea se numără categoriile de motive ale refuzului intrării și al șederii și detaliile privind documentele de identificare personale ale persoanelor vizate. Aceste informații mai ample permit, pe de o parte, o mai bună identificare a persoanei vizate și, pe de altă parte, luarea de către utilizatorii finali a unei decizii în cunoștință de cauză, pe baza mai multor elemente. Pentru protecția utilizatorilor finali care efectuează verificările, SIS va indica, de asemenea, dacă persoana care face obiectul unei semnalări se încadrează în vreuna dintre categoriile

prevăzute la articolele 1, 2, 3 și 4 din Decizia-cadru 2002/475/JAI a Consiliului privind combaterea terorismului[33].

Propunerea clarifică faptul că statele membre nu trebuie să copieze datele introduse de un alt stat membru în alte fișiere de date naționale (articolul 37).

Păstrarea

Articolul 34 stabilește termenul de reexaminare a semnalărilor. Perioada maximă de păstrare a semnalărilor privind refuzul intrării și al șederii a fost aliniată la termenul cel mai îndelungat posibil al interdicțiilor de intrare emise în conformitate cu articolul 11 din Directiva 2008/115/CE. Prin urmare, perioada maximă de păstrare va fi de 5 ani; cu toate acestea, statele membre pot stabili perioade mai scurte.

Ștergerea

Articolul 35 stabilește circumstanțele în care semnalările trebuie șterse, ceea ce duce la o armonizare sporită a practicilor naționale din acest domeniu. Articolul 35 stabilește dispoziții speciale pentru personalul biroului SIRENE privind ștergerea în mod proactiv a semnalărilor care nu mai sunt necesare, dacă nu se primește niciun răspuns din partea autorităților competente.

Drepturile persoanelor vizate privind accesul la date, rectificarea datelor inexacte și ștergerea datelor stocate în mod ilegal

Normele detaliate privind drepturile persoanei vizate au rămas neschimbate, deoarece normele existente asigură deja un nivel ridicat de protecție și sunt conforme cu Regulamentul (UE) 2016/679[34] și cu Directiva 2016/680[35]. În plus, articolul 48 stabilește circumstanțele în care statele membre pot decide să nu comunice informații persoanelor vizate. Acest refuz trebuie să fie justificat de unul dintre motivele enumerate la articolul menționat și trebuie să fie o măsură proporțională și necesară, în concordanță cu dreptul național.

Statistici

Pentru a menține o imagine de ansamblu asupra funcționării căilor de atac, articolul 49 prevede un sistem statistic standard de raportare anuală privind numărul de:

- cereri de acces ale persoanelor vizate;
- cereri de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal;
- cauze soluționate de o instanță judecătorească;

---

33 Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO L 164, 22.6.2002, p. 3).

34 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).

35 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 (JO L 119, 4.5.2016, p. 89).

- cauze în care o instanță judecătorească s-a pronunțat în favoarea reclamantului și
- observații privind cazurile de recunoaștere reciprocă a deciziilor definitive pronunțate de instanțele judecătorești sau de autoritățile altor state membre privind semnalările create de statul membru care a emis semnalarea.

Monitorizare și statistici

Articolul 54 stabilește mecanismele care trebuie instituite pentru a se asigura monitorizarea corespunzătoare a SIS și funcționarea sa în raport cu obiectivele sale. În acest scop, eu-LISA este însărcinată cu furnizarea de statistici zilnice, lunare și anuale privind modul în care este utilizat sistemul.

Articolul 54 alineatul (5) prevede obligația eu-LISA de a furniza statelor membre, Comisiei, Europol și Agenției Europene pentru Poliția de Frontieră și Garda de Coastă rapoartele statistice pe care le elaborează și autorizează Comisia să solicite rapoarte statistice suplimentare și rapoarte suplimentare privind calitatea datelor referitoare la SIS și la comunicațiile SIRENE.

Articolul 54 alineatul (6) prevede înființarea și găzduirea unui registru central de date în cadrul activității eu-LISA privind monitorizarea funcționării SIS. Acest lucru va permite personalului autorizat din statele membre, Comisiei, Europol și Agenției Europene pentru Poliția de Frontieră și Garda de Coastă să aibă acces la datele enumerate la articolul 54 alineatul (3) în vederea întocmirii statisticilor necesare.

2016/0408 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Regulamentului (UE) nr. 515/2014 și de abrogare a Regulamentului (CE) nr. 1987/2006

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 77 alineatul (2) literele (b) și (d) și articolul 79 alineatul (2) litera (c),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Sistemul de informații Schengen (SIS) este un instrument esențial pentru aplicarea dispozițiilor acquis-ului Schengen, astfel cum este integrat acesta în cadrul Uniunii Europene. SIS este una dintre măsurile compensatorii majore care contribuie la menținerea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție al Uniunii Europene, prin sprijinirea cooperării operaționale dintre polițiștii de frontieră, poliție, autoritățile vamale și alte autorități de asigurare a respectării legii, autoritățile judiciare în materie penală și autoritățile din domeniul imigrației.

(2) SIS a fost instituit în temeiul dispozițiilor titlului IV din Convenția din 19 iunie 1990 de punere în aplicare a acordului Schengen din 14 iunie 1985 dintre guvernele statelor din Uniunea Economică Benelux, Republicii Federale Germania și Republicii Franceze privind eliminarea treptată a controalelor la frontierele comune[36] (Convenția Schengen). Dezvoltarea SIS de a doua generație (SIS II) a fost încredințată Comisiei în temeiul Regulamentului (CE) nr. 2424/2001 al Consiliului[37] și al Deciziei 2001/886/JAI a Consiliului (SIS)[38] și acest sistem a fost instituit prin Regulamentul (CE) nr. 1987/2006[39], precum și prin Decizia 2007/533/JAI a Consiliului[40]. SIS II a înlocuit SIS, astfel cum a fost creat în temeiul Convenției Schengen.

---

36 JO L 239, 22.9.2000, p. 19. Convenție astfel cum a fost modificată prin Regulamentul (CE) nr. 1160/2005 al Parlamentului European și al Consiliului (JO L 191, 22.7.2005, p. 18).

37 JO L 328, 13.12.2001, p. 4.

38 Decizia 2001/886/JAI a Consiliului din 6 decembrie 2001 privind dezvoltarea Sistemului de Informații Schengen din a doua generație (SIS II) (JO L 328, 13.12.2001, p. 1).

39 Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație (SIS II) (JO L 181, 28.12.2006, p. 4).

(3) La trei ani după intrarea în funcțiune a SIS II, Comisia a efectuat o evaluare a sistemului în conformitate cu articolul 24 alineatul (5), articolul 43 alineatul (5) și articolul 50 alineatul (5) din Regulamentul (CE) nr. 1987/2006 și cu articolul 59 și articolul 65 alineatul (5) din Decizia 2007/533/JAI. Raportul de evaluare și documentul de lucru conex au fost adoptate la 21 decembrie 2016[41]. Recomandările formulate în aceste documente ar trebui să se reflecte, după caz, în prezentul regulament.

(4) Prezentul regulament constituie temeiul juridic necesar pentru reglementarea SIS în ceea ce privește aspectele care intră în domeniul de aplicare al titlului V capitolul 2 din Tratatul privind funcționarea Uniunii Europene. Regulamentul (UE) 2018/... al Parlamentului European și al Consiliului privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală[42] constituie temeiul juridic necesar pentru reglementarea SIS în ceea ce privește aspectele care intră în domeniul de aplicare al titlului V capitolele 4 și 5 din Tratatul privind funcționarea Uniunii Europene.

(5) Faptul că temeiul juridic necesar pentru reglementarea SIS constă în instrumente separate nu afectează principiul conform căruia SIS constituie un sistem de informații unic, care ar trebui să funcționeze ca atare. Prin urmare, anumite dispoziții ale acestor instrumente ar trebui să fie identice.

(6) Este necesar să se specifice obiectivele SIS, arhitectura tehnică și finanțarea acestuia, să se stabilească norme privind funcționarea și utilizarea acestuia de la un capăt la altul (*end-to-end*) și să se definească responsabilitățile, categoriile de date care trebuie introduse în sistem, scopurile și criteriile introducerii acestora, autoritățile autorizate să aibă acces la date, utilizarea elementelor biometrice de identificare și alte norme privind prelucrarea datelor.

(7) SIS cuprinde un sistem central (SIS central) și sisteme naționale cu o copie integrală sau parțială a bazei de date din SIS. Având în vedere faptul că SIS este cel mai important instrument de schimb de informații în Europa, este necesar să se asigure funcționarea neîntreruptă a acestuia, atât la nivel central, cât și la nivel național. Prin urmare, fiecare stat membru ar trebui să realizeze o copie parțială sau integrală a bazei de date din SIS și ar trebui să înființeze un sistem propriu de rezervă.

(8) Este necesar să se mențină un manual care să stabilească normele detaliate privind schimbul de anumite informații suplimentare referitoare la acțiunea care trebuie întreprinsă ca urmare a semnalărilor. Autoritățile naționale din fiecare stat membru (birourile SIRENE) ar trebui să asigure schimbul acestor informații.

(9) Pentru a se menține schimbul eficient de informații suplimentare privind acțiunea care trebuie întreprinsă specificată în semnalări, este oportun să se consolideze funcționarea birourilor SIRENE prin precizarea cerințelor referitoare la resursele disponibile, formarea utilizatorilor și timpul de răspuns la solicitările primite din partea altor birouri SIRENE.

---

[40] 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).

[41] Raportul către Parlamentul European și Consiliu privind evaluarea Sistemului de informații Schengen de a doua generație (SIS II) în conformitate cu articolul 24 alineatul (5), articolul 43 alineatul (3) și articolul 50 alineatul (5) din Regulamentul (CE) nr. 1987/2006 și cu articolul 59 alineatul (3) și articolul 66 alineatul (5) din Decizia 2007/533/JAI și documentul de lucru însoțitor

[42] Regulamentul (UE) 2018/…

(10) Gestionarea operațională a componentelor centrale ale SIS este efectuată de Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție[43] („agenția”). Pentru a permite agenției să aloce resursele financiare și de personal necesare care să acopere toate aspectele legate de gestionarea operațională a SIS central, prezentul regulament ar trebui să îi stabilească în detaliu sarcinile, în special în ceea ce privește aspectele tehnice ale schimbului de informații suplimentare.

(11) Fără a aduce atingere responsabilității statelor membre pentru exactitatea datelor introduse în SIS, agenția ar trebui să devină responsabilă cu îmbunătățirea calității datelor, prin introducerea unui instrument central de monitorizare a calității datelor, și cu furnizarea de rapoarte statelor membre, la intervale regulate.

(12) Pentru a permite o mai bună monitorizare a utilizării SIS în scopul de a analiza tendințele privind presiunea migrației și gestionarea frontierelor, agenția ar trebui să fie în măsură să dezvolte un sistem conform cu stadiul actual al tehnologiei în vederea elaborării de rapoarte statistice destinate statelor membre, Comisiei, Europol și Agenției Europene pentru Poliția de Frontieră și Garda de Coastă fără a pune în pericol integritatea datelor. Prin urmare, ar trebui să se instituie un registru statistic central. Orice statistică întocmită nu ar trebui să conțină date cu caracter personal.

(13) SIS ar trebui să conțină categorii suplimentare de date pentru a permite utilizatorilor finali să ia decizii în cunoștință de cauză pe baza unei semnalări, fără a pierde timp. Prin urmare, semnalările în scopul refuzării intrării și a șederii ar trebui să conțină informații privind decizia pe care se bazează semnalarea. În plus, pentru a facilita identificarea și a depista identitățile multiple, semnalarea ar trebui să includă o trimitere la documentul de identificare personal sau la numărul acestuia și o copie a documentului respectiv, în cazul în care sunt disponibile.

(14) SIS nu ar trebui să stocheze date utilizate pentru efectuarea de căutări, cu excepția păstrării înregistrărilor cu scopul de a verifica dacă respectiva căutare efectuată în date este legală, de a monitoriza legalitatea prelucrării datelor, de a efectua automonitorizarea și de a asigura funcționarea corespunzătoare a N.SIS, precum și integritatea și securitatea datelor.

(15) SIS ar trebui să permită prelucrarea datelor biometrice pentru a facilita identificarea fiabilă a persoanelor în cauză. În aceeași perspectivă, SIS ar trebui, de asemenea, să permită prelucrarea datelor privind persoanele a căror identitate a fost uzurpată (pentru a evita inconvenientele cauzate de identificarea eronată a acestora), sub rezerva unor garanții adecvate, în special cu acordul persoanei în cauză și cu o limitare strictă a scopurilor în care aceste date pot fi prelucrate în mod legal.

(16) Statele membre ar trebui să ia măsurile tehnice necesare astfel încât de fiecare dată când utilizatorii finali au dreptul de a efectua o căutare într-o bază de date națională a poliției sau în materie de imigrație, aceștia să efectueze, de asemenea, în paralel căutări în SIS, în conformitate cu articolul 4 din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului[44]. Acest lucru ar trebui să asigure că SIS

---

[43] Instituită prin Regulamentul (UE) nr. 1077/2011 al Parlamentului European și al Consiliului din 25 octombrie 2011 de instituire a Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (JO L 286, 1.11.2011, p. 1).

[44] 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

funcționează ca principala măsură compensatorie în spațiul fără controale la frontierele interne și să abordeze mai bine dimensiunea transfrontalieră a criminalității și mobilitatea infractorilor.

(17) Prezentul regulament ar trebui să prevadă condițiile de utilizare a datelor dactiloscopice și a imaginilor faciale în scopul identificării. Utilizarea în SIS a imaginilor faciale în scopul identificării ar trebui, de asemenea, să contribuie la asigurarea coerenței în cadrul procedurilor de control la frontiere în cazul în care sunt necesare identificarea și verificarea identității cu ajutorul datelor dactiloscopice și al imaginilor faciale. Efectuarea de căutări cu ajutorul datelor dactiloscopice ar trebui să fie obligatorie în cazul în care există vreo îndoială privind identitatea unei persoane. Imaginile faciale ar trebui utilizate în scopul identificării doar în contextul controalelor obișnuite la frontiere în chioșcurile de control self-service și la porțile electronice.

(18) Amprentele digitale găsite la locul unei infracțiuni ar trebui să poată fi confruntate cu datele dactiloscopice stocate în SIS, dacă se poate stabili cu un grad ridicat de probabilitate că acestea aparțin autorului unei infracțiuni grave sau al unei infracțiuni de terorism. Infracțiuni grave ar trebui să fie infracțiunile menționate în Decizia-cadru 2002/584/JAI a Consiliului[45] și „infracțiune de terorism” ar trebui să fie infracțiunile prevăzute de dreptul național menționate în Decizia-cadru 2002/475/JAI a Consiliului[46].

(19) Statele membre ar trebui să poată stabili conexiuni între semnalările din SIS. Stabilirea de către un stat membru a unor conexiuni între două sau mai multe semnalări nu ar trebui să aibă efect asupra acțiunii care trebuie întreprinsă, asupra perioadei de păstrare a semnalărilor sau asupra drepturilor de acces la semnalări.

(20) Un nivel mai ridicat de eficacitate, armonizare și coerență se poate realiza prin impunerea obligației de a introduce în SIS toate interdicțiile de intrare emise de autoritățile competente din statele membre în conformitate cu proceduri care respectă Directiva 2008/115/CE[47] și prin stabilirea de norme comune pentru introducerea acestor semnalări în urma returnării resortisantului țării terțe aflat în situație de ședere ilegală. Statele membre ar trebui să ia toate măsurile necesare pentru a se asigura că nu există un decalaj temporar între momentul părăsirii spațiului Schengen de către resortisantul țării terțe și activarea în SIS a semnalării. Acest fapt ar trebui să garanteze asigurarea cu succes a respectării interdicțiilor de intrare la punctele de trecere a frontierelor externe, prevenind în mod eficace reintrarea în spațiul Schengen.

(21) Prezentul regulament ar trebui să stabilească norme obligatorii privind consultarea autorităților naționale în cazul în care un resortisant al unei țări terțe deține sau poate obține un permis de ședere valabil sau o altă autorizație ori un drept de ședere acordat într-un stat membru și un alt stat membru intenționează să emită sau a introdus deja o semnalare privind refuzul intrării și al șederii pentru resortisantul țării terțe în cauză. Aceste situații creează incertitudini grave pentru polițiștii de frontieră, pentru poliție și

---

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).

45 Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (JO L 190, 18.7.2002, p. 1).

46 Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO L 164, 22.6.2002, p. 3).

47 Directiva 2008/115/CE a Parlamentului European și a Consiliului din 16 decembrie 2008 privind standardele și procedurile comune aplicabile în statele membre pentru returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală (JO L 348, 24.12.2008, p. 98).

pentru autoritățile din domeniul imigrației. Prin urmare, este oportun să se prevadă un termen obligatoriu de consultare rapidă cu un rezultat precis pentru a se evita ca persoanele care reprezintă o amenințare să poată intra în spațiul Schengen.

(22) Prezentul regulament nu ar trebui să aducă atingere aplicării Directivei 2004/38/CE[48].

(23) Semnalările nu ar trebui păstrate în SIS mai mult timp decât este necesar în vederea îndeplinirii scopurilor pentru care au fost emise. În vederea reducerii sarcinii administrative suportate de autoritățile implicate în prelucrarea datelor privind persoane în diferite scopuri, este oportun să se alinieze perioada maximă de păstrare a semnalărilor privind refuzul intrării și al șederii cu durata maximă posibilă a interdicțiilor de intrare emise în conformitate cu proceduri care respectă Directiva 2008/115/CE. Prin urmare, perioada de păstrare a semnalărilor privind persoane ar trebui să fie de maximum cinci ani. Ca principiu general, semnalările privind persoane trebuie șterse în mod automat din SIS după o perioadă de cinci ani. Deciziile de a păstra semnalări privind persoane ar trebui să se bazeze pe o evaluare individuală cuprinzătoare. Statele membre ar trebui să reexamineze semnalările privind persoane în termenul stabilit și să întocmească statistici referitoare la numărul de semnalări privind persoane în cazul cărora care s-a prelungit perioada de păstrare.

(24) Introducerea și prelungirea în SIS a datei de expirare a valabilității unei semnalări ar trebui să facă obiectul cerinței de proporționalitate necesare, examinându-se dacă un caz concret este suficient de adecvat, relevant și important pentru a se introduce o semnalare în SIS. În cazul infracțiunilor prevăzute la articolele 1, 2, 3 și 4 din Decizia-cadru 2002/475/JAI a Consiliului privind combaterea terorismului[49], ar trebui să se creeze întotdeauna o semnalare privind resortisanții țărilor terțe în scopul refuzării intrării și a șederii, ținând seama de nivelul ridicat de amenințare și impactul negativ global pe care îl poate genera o astfel de activitate.

(25) Integritatea datelor din SIS are o importanță majoră. Prin urmare, ar trebui prevăzute garanții corespunzătoare pentru prelucrarea datelor din SIS atât la nivel central, cât și la nivel național, în vederea asigurării securității datelor de la un capăt la altul. Autoritățile implicate în prelucrarea datelor ar trebui să respecte cerințele de securitate prevăzute în prezentul regulament și să aplice o procedură uniformă de raportare a incidentelor.

(26) Datele prelucrate în SIS în conformitate cu prezentul regulament nu ar trebui să fie transferate sau puse la dispoziția țărilor terțe sau a organizațiilor internaționale.

(27) Pentru a spori eficiența activității autorităților din domeniul imigrației atunci când decid cu privire la dreptul resortisanților țărilor terțe de a intra și a rămâne pe teritoriul statelor membre, precum și cu privire la returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală, este oportun să se acorde acestor autorități acces la SIS prin prezentul regulament.

(28) Regulamentul (UE) 2016/679[50] ar trebui să se aplice prelucrării datelor cu caracter personal în temeiul prezentului regulament de către autoritățile statelor membre atunci

---

48 Directiva 2004/38/CE a Parlamentului European și a Consiliului din 29 aprilie 2004 privind dreptul la liberă circulație și ședere pe teritoriul statelor membre pentru cetățenii Uniunii și membrii familiilor acestora (JO L 158, 30.4.2004, p. 77).

49 Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO L 164, 22.6.2002, p. 3).

50 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

când nu se aplică Directiva (UE) 2016/680[51]. Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului[52] ar trebui să se aplice prelucrării datelor cu caracter personal de către instituțiile și organele Uniunii atunci când își exercită responsabilitățile care le revin în temeiul prezentului regulament. Dispozițiile Directivei (UE) 2016/680, ale Regulamentului (UE) 2016/679 și ale Regulamentului (CE) nr. 45/2001 ar trebui să fie detaliate în prezentul regulament, în cazul în care este necesar. În ceea ce privește prelucrarea datelor cu caracter personal de către Europol, se aplică Regulamentul (UE) 2016/794 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii[53] (Regulamentul privind Europol).

(29) În ceea ce privește confidențialitatea, funcționarii sau alți agenți care sunt angajați și își desfășoară activitatea în legătură cu SIS ar trebui să se supună dispozițiilor corespunzătoare din Statutul funcționarilor Uniunii Europene și din Regimul aplicabil celorlalți agenți ai Uniunii Europene.

(30) Atât statele membre, cât și agenția ar trebui să mențină planuri de securitate pentru a facilita punerea în aplicare a obligațiilor privind securitatea și ar trebui să coopereze între ele pentru a aborda aspectele legate de securitate dintr-o perspectivă comună.

(31) Autoritățile naționale independente de supraveghere ar trebui să monitorizeze legalitatea prelucrării datelor cu caracter personal în legătură cu prezentul regulament de către statele membre. Ar trebui să se stabilească drepturile persoanelor vizate de acces, rectificare și ștergere a datelor lor cu caracter personal stocate în SIS și căile de atac ulterioare în fața instanțelor judecătorești naționale, precum și recunoașterea reciprocă a hotărârilor judecătorești. Prin urmare, este oportun să se solicite statistici anuale din partea statelor membre.

(32) Autoritățile naționale de supraveghere ar trebui să se asigure că cel puțin din patru în patru ani se efectuează un audit al operațiunilor de prelucrare a datelor în sistemul lor N.SIS în conformitate cu standardele internaționale de audit. Auditul ar trebui să fie efectuat de autoritățile de supraveghere sau autoritățile naționale de supraveghere ar trebui să dispună în mod direct efectuarea auditului de către un auditor independent în materie de protecție a datelor. Auditorul independent ar trebui să rămână sub controlul și responsabilitatea autorității sau autorităților naționale de supraveghere care, prin urmare, ar trebui să dispună ea (ele) însăși (însele) auditul și să definească în mod clar scopul, domeniul de aplicare și metodologia auditului, precum și să ofere îndrumări și să asigure supravegherea auditului și a rezultatelor finale ale acestuia.

(33) Regulamentul (UE) 2016/794 (Regulamentul privind Europol) prevede că Europol susține și consolidează acțiunile întreprinse de autoritățile competente ale statelor membre și cooperarea acestora în vederea combaterii terorismului și a altor forme

---

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).

[51] 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 (JO L 119, 4.5.2016, p. 89).

[52] 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).

[53] Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului (JO L 135, 25.5.2016, p. 53).

grave de criminalitate și furnizează analize și evaluări ale amenințărilor. Pentru a facilita îndeplinirea de către Europol a sarcinilor care îi revin, în special în cadrul Centrului european privind introducerea ilegală de migranți, este oportun să se permită accesul Europol la categoriile de semnalări definite în prezentul regulament. Centrul european privind introducerea ilegală de migranți din cadrul Europol, care joacă un rol strategic fundamental în combaterea facilitării migrației neregulamentare, ar trebui să aibă acces la semnalările privind persoanele cărora li s-a refuzat intrarea și șederea pe teritoriul unui stat membru din motive ce țin de dreptul penal sau din cauza nerespectării condițiilor de intrare și de ședere.

(34) În vederea eliminării lacunelor din domeniul schimbului de informații privind terorismul, în special privind luptătorii teroriști străini, în cazul în care monitorizarea deplasărilor acestora este extrem de importantă, statele membre ar trebui să facă schimb de informații privind activitățile legate de terorism cu Europol, în paralel cu introducerea unei semnalări în SIS, precum și privind rezultatele pozitive și informațiile conexe. Acest lucru ar trebui să permită Centrului european de combatere a terorismului din cadrul Europol să verifice dacă în bazele de date ale Europol există informații contextuale suplimentare și să furnizeze analize de înaltă calitate care să contribuie la destrămarea rețelelor teroriste și, dacă este posibil, la prevenirea atacurilor acestora.

(35) Este necesar, de asemenea, să se stabilească norme clare privind prelucrarea și descărcarea datelor din SIS de către Europol pentru a permite o utilizare cât mai cuprinzătoare a SIS, cu condiția ca standardele de protecție a datelor să fie respectate, astfel cum se prevede în prezentul regulament și în Regulamentul (UE) 2016/794. În cazurile în care căutările efectuate în SIS de Europol indică existența unei semnalări emise de un stat membru, Europol nu poate lua măsurile necesare. Prin urmare, acesta ar trebui să informeze statul membru în cauză care să îl autorizeze să se ocupe de caz.

(36) Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului[54] prevede, în sensul prezentului regulament, că statul membru gazdă îi autorizează pe membrii echipelor europene de poliție de frontieră și gardă de coastă sau ai echipelor de personal implicat în sarcini legate de returnare, trimise de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă, să consulte bazele de date europene, în cazul în care această consultare este necesară pentru îndeplinirea obiectivelor operative specificate în planul operativ privind verificările la frontieră, supravegherea frontierelor și returnare. Alte agenții relevante ale Uniunii, în special Biroul European de Sprijin pentru Azil și Europol, pot, de asemenea, să trimită în cadrul echipelor de sprijin pentru gestionarea migrației experți care nu sunt membri ai personalului respectivelor agenții ale Uniunii. Obiectivul trimiterii echipelor europene de poliție de frontieră și gardă de coastă, a echipelor de personal implicat în sarcini legate de returnare și a echipelor de sprijin pentru gestionarea migrației este de a oferi întăriri tehnice și operative statelor membre solicitante, în special celor care se confruntă cu provocări disproporționate legate de migrație. În vederea îndeplinirii sarcinilor atribuite echipelor europene de poliție de frontieră și gardă de coastă, echipelor de personal implicat în sarcini legate de returnare și echipelor de sprijin pentru

[54] 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).

gestionarea migrației este necesar accesul la SIS prin intermediul unei interfețe tehnice a Agenției Europene pentru Poliția de Frontieră și Garda de Coastă care să se conecteze la SIS central. În cazul în care căutările efectuate în SIS de echipa sau de echipele de personal indică existența unei semnalări emise de un stat membru, membrul echipei sau personalul nu poate întreprinde acțiunea necesară, cu excepția cazului în care este autorizat în acest sens de statul membru gazdă. Prin urmare, acesta ar trebui să informeze statul membru în cauză care să îl autorizeze să se ocupe de caz.

(37) În conformitate cu Regulamentul (UE) 2016/1624, Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă elaborează analize de risc. Aceste analize de risc acoperă toate aspectele relevante pentru gestionarea europeană integrată a frontierelor, în special amenințările susceptibile să afecteze funcționarea sau securitatea frontierelor externe. Semnalările introduse în SIS în conformitate cu prezentul regulament, în special semnalările privind refuzul intrării și al șederii, constituie informații relevante pentru evaluarea eventualelor amenințări care pot afecta frontierele externe și ar trebui, prin urmare, să fie disponibile în vederea analizei de risc care trebuie să fie elaborată de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă. Pentru îndeplinirea sarcinilor atribuite Agenției Europene pentru Poliția de Frontieră și Garda de Coastă în ceea ce privește analiza de risc este necesar accesul la SIS. De asemenea, în conformitate cu Propunerea Comisiei de regulament al Parlamentului European și al Consiliului de instituire a unui sistem european de informații și de autorizare privind călătoriile (ETIAS)[55], unitatea centrală a ETIAS din cadrul Agenției Europene pentru Poliția de Frontieră și Garda de Coastă va efectua verificări în SIS, prin intermediul ETIAS, pentru a analiza cererile de autorizații de călătorie în cazul cărora este necesar, printre altele, să se stabilească dacă resortisantul țării terțe care solicită o autorizație de călătorie face obiectul unei semnalări în SIS. În acest scop, unitatea centrală a ETIAS din cadrul Agenției Europene pentru Poliția de Frontieră și Garda de Coastă ar trebui, de asemenea, să aibă acces la SIS, în măsura necesară în vederea îndeplinirii mandatului său, și anume la toate categoriile de semnalări privind resortisanții țărilor terțe pentru care s-a emis o semnalare privind intrarea și șederea, precum și care fac obiectul unei măsuri restrictive menite să împiedice intrarea pe teritoriile statelor membre sau tranzitarea acestor teritorii.

(38) Dată fiind natura lor tehnică, gradul lor de detaliu și necesitatea de a fi actualizate în mod regulat, anumite aspecte ale SIS nu pot fi reglementate în mod exhaustiv de dispozițiile prezentului regulament. Printre acestea se numără, de exemplu, normele tehnice privind introducerea, actualizarea și ștergerea datelor și efectuarea de căutări în date, calitatea datelor și normele de căutare referitoare la elementele biometrice de identificare, normele privind compatibilitatea și prioritatea semnalărilor, adăugarea indicatorilor de validitate, conexiunile dintre semnalări, stabilirea datei de expirare a valabilității semnalărilor în termenul maxim și schimbul de informații suplimentare. Prin urmare, Comisiei ar trebui să i se confere competențe de executare cu privire la aceste aspecte. Normele tehnice privind efectuarea de căutări în semnalări ar trebui să ia în considerare buna funcționare a aplicațiilor naționale.

(39) Pentru a se asigura condiții uniforme de punere în aplicare a prezentului regulament, Comisiei ar trebui să i se confere competențe de executare. Aceste competențe ar

[55] COM (2016) 731 final.

trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011[56]. Procedura de adoptare a măsurilor de punere în aplicare în temeiul prezentului regulament și al Regulamentului (UE) 2018/xxx (cooperarea polițienească și judiciară) ar trebui să fie aceeași.

(40) Pentru a se asigura transparența, agenția ar trebui să elaboreze din doi în doi ani un raport privind funcționarea tehnică a SIS central și privind funcționarea infrastructurii de comunicare, inclusiv securitatea acesteia, și privind schimbul de informații suplimentare. Comisia ar trebui să efectueze o evaluare globală din patru în patru ani.

(41) Deoarece obiectivele prezentului regulament, și anume instituirea și reglementarea unui sistem de informații comun și schimbul de informații suplimentare conexe, nu pot, prin însăși natura lor, să fie realizate într-o măsură suficientă de statele membre și, în consecință, pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul menționat, prezentul regulament nu depășește ceea ce este necesar pentru realizarea acestor obiective.

(42) Prezentul regulament respectă drepturile fundamentale și principiile recunoscute în special în Carta drepturilor fundamentale a Uniunii Europene. În special, prezentul regulament vizează să asigure un mediu sigur pentru toate persoanele care locuiesc pe teritoriul Uniunii Europene și protecția migranților în situație neregulamentară împotriva exploatării și a traficului de persoane prin permiterea identificării lor, respectând în același timp pe deplin protecția datelor cu caracter personal.

(43) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la TFUE, 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 menționat, în termen de șase luni de la data la care Consiliul hotărăște cu privire la prezentul regulament, dacă îl va transpune în legislația sa națională.

(44) 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[57]; prin urmare, Regatul Unit nu participă la adoptarea prezentului regulament, nu are obligații în temeiul acestuia și nu face obiectul aplicării sale.

(45) Prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen la care Irlanda nu participă, în conformitate cu Decizia 2002/192/CE a Consiliului[58] ; prin urmare, Irlanda nu participă la adoptarea prezentului regulament, nu are obligații în temeiul acestuia și nu face obiectul aplicării sale.

(46) În ceea ce privește Islanda și Norvegia, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen în sensul Acordului încheiat de Consiliul Uniunii Europene și Republica Islanda și Regatul Norvegiei privind asocierea acestora din

---

56 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).

57 JO L 131, 1.6.2000, p. 43.

58 JO L 64, 7.3.2002, p. 20.

urmă la implementarea, aplicarea și dezvoltarea acquis-ului Schengen[59], care intră sub incidența domeniului menționat la articolul 1 punctul G din Decizia 1999/437/CE a Consiliului[60] privind anumite modalități de aplicare a acordului menționat.

(47) În ceea ce privește Elveția, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen în sensul Acordului semnat între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la transpunerea, punerea în aplicare și dezvoltarea acquis-ului Schengen, care intră sub incidența domeniului menționat la articolul 1 punctul G din Decizia 1999/437/CE a Consiliului, coroborat cu articolul 4 alineatul (1) din Deciziile 2004/849/CE[61] și 2004/860/CE[62] ale Consiliului.

(48) În ceea ce privește Liechtenstein, prezenta decizie constituie o dezvoltare a dispozițiilor acquis-ului Schengen în sensul Protocolului dintre Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în practică, aplicarea și dezvoltarea acquis-ului Schengen[63], care intră sub incidența domeniului menționat la articolul 1 punctul G din Decizia 1999/437/CE, coroborat cu articolul 3 din Decizia 2011/349/UE a Consiliului[64] și cu articolul 3 din Decizia 2011/350/UE a Consiliului[65].

(49) În ceea ce privește Bulgaria și România, prezentul regulament constituie un act care se întemeiază pe acquis-ul Schengen sau care este conex acestuia în sensul articolului 4 alineatul (2) din Actul de aderare din 2005 și ar trebui coroborat cu Decizia 2010/365/UE a Consiliului privind aplicarea dispozițiilor acquis-ului Schengen referitoare la Sistemul de Informații Schengen în Republica Bulgaria și în România[66].

(50) În ceea ce privește Cipru și Croația, prezentul regulament constituie un act care se întemeiază pe acquis-ul Schengen sau care este conex acestuia, în sensul articolului 3

---

59 JO L 176, 10.7.1999, p. 36.

60 JO L 176, 10.7.1999, p. 31.

61 Decizia 2004/849/CE a Consiliului din 25 octombrie 2004 privind semnarea, în numele Uniunii Europene, și aplicarea provizorie a anumitor dispoziții ale Acordului dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la transpunerea, punerea în aplicare și dezvoltarea acquis-ului Schengen (JO L 368, 15.12.2004, p. 26).

62 Decizia 2004/860/CE a Consiliului din 25 octombrie 2004 referitoare la semnarea, în numele Comunității Europene, și la aplicarea provizorie a anumitor dispoziții ale Acordului dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, asigurarea respectării și dezvoltarea acquis-ului Schengen (JO L 370, 17.12.2004, p. 78).

63 JO L 160, 18.6.2011, p. 21.

64 Decizia 2011/349/UE a Consiliului din 7 martie 2011 privind încheierea, în numele Uniunii Europene, a Protocolului dintre Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen, în special în ceea ce privește cooperarea judiciară în materie penală și cooperarea polițienească (JO L 160, 18.6.2011, p. 1).

65 Decizia 2011/350/UE a Consiliului din 7 martie 2011 privind încheierea, în numele Uniunii Europene, a Protocolului dintre Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen, în ceea ce privește eliminarea controalelor la frontierele interne și circulația persoanelor (JO L 160, 18.6.2011, p. 19).

66 JO L 166, 1.7.2010, p. 17.

alineatul (2) din Actul de aderare din 2003 și, respectiv, al articolului 4 alineatul (2) din Actul de aderare din 2011.

(51) Costurile estimate privind actualizarea sistemelor naționale SIS și punerea în aplicare a noilor funcționalități, prevăzute în prezentul regulament, sunt mai mici decât suma rămasă la linia bugetară pentru frontiere inteligente din Regulamentul (UE) nr. 515/2014 al Parlamentului European și al Consiliului[67]. Prin urmare, prezentul regulament ar trebui să realoce, în conformitate cu articolul 5 alineatul (5) litera (b) din Regulamentul (UE) nr. 515/2014, suma atribuită dezvoltării de sisteme informatice pentru gestionarea fluxurilor migratorii la frontierele externe.

(52) Prin urmare, Regulamentul (CE) nr. 1987/2006 ar trebui abrogat.

(53) 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 …,

[67] 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 (JO L 150, 20.5.2014, p. 143).

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1
Scopul general al SIS

Scopul SIS este de a asigura un 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 teritoriile statelor membre, și de a aplica dispozițiile părții a treia titlul V capitolul 2 din Tratatul privind funcționarea Uniunii Europene referitoare la circulația persoanelor pe teritoriile statelor membre, cu ajutorul informațiilor transmise prin intermediul acestui sistem.

Articolul 2
Domeniul de aplicare

1. Prezentul regulament stabilește condițiile și procedurile referitoare la introducerea și prelucrarea în SIS a semnalărilor privind resortisanții țărilor terțe, precum și la schimbul de informații suplimentare și date suplimentare în scopul refuzării intrării și a șederii pe teritoriul statelor membre.

2. Prezentul regulament stabilește, de asemenea, dispoziții privind arhitectura tehnică a SIS, responsabilitățile statelor membre și ale Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție, norme generale de prelucrare a datelor, drepturile persoanelor vizate și răspunderea.

Articolul 3
Definiții

1. În sensul prezentului regulament, se aplică următoarele definiții:

   (a) „semnalare” înseamnă un set de date, inclusiv elementele biometrice de identificare astfel cum sunt menționate la articolul 22, introduse în SIS care permit autorităților competente să identifice o persoană în vederea întreprinderii unei acțiuni specifice;

   (b) „informații suplimentare” înseamnă informațiile care nu fac parte din datele semnalării stocate în SIS, dar au legătură cu semnalările din SIS, și care urmează a fi transmise în cadrul unui schimb de informații:

      (1) pentru a permite statelor membre să se consulte sau să se informeze reciproc la introducerea unei semnalări;

      (2) pentru a permite întreprinderea acțiunii corespunzătoare în urma obținerii unui rezultat pozitiv (*hit*);

      (3) în cazul în care nu se poate întreprinde acțiunea necesară;

      (4) în ceea ce privește calitatea datelor din SIS;

(5) în ceea ce privește compatibilitatea și ordinea de prioritate a semnalărilor;

(6) în ceea ce privește drepturile de acces;

(c) „date suplimentare” înseamnă datele stocate în SIS care au legătură cu semnalările din SIS și care trebuie să fie puse imediat la dispoziția autorităților competente în cazul în care o persoană cu privire la care s-au introdus date în SIS este localizată ca urmare a căutărilor efectuate în acest sistem;

(d) „resortisant al unei țări terțe” înseamnă orice persoană care nu este cetățean al Uniunii în sensul articolului 20 din TFUE, cu excepția persoanelor care beneficiază de drepturi de liberă circulație echivalente cu cele ale cetățenilor Uniunii în temeiul acordurilor dintre Uniune sau dintre Uniune și statele sale membre, pe de o parte, și țările terțe, pe de altă parte;

(e) „date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoană vizată”);

(f) „persoană fizică identificabilă” înseamnă o persoană fizică ce poate fi identificată, în mod direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare ori un identificator online, sau la unul ori mai multe elemente specifice identității fizice, fiziologice, genetice, mentale, economice, culturale sau sociale ale respectivei persoane fizice;

(g) „prelucrarea datelor cu caracter personal” înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminare sau punere la dispoziție în alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

(h) „rezultat pozitiv” (*hit*) în SIS înseamnă că:

(1) un utilizator efectuează o căutare;

(2) căutarea indică o semnalare introdusă în SIS de un alt stat membru;

(3) datele privind semnalarea din SIS corespund datelor căutării și

(4) în urma obținerii rezultatului pozitiv, trebuie întreprinse acțiuni suplimentare;

(i) „stat membru semnalant” înseamnă statul membru care a introdus semnalarea în SIS;

(j) „stat membru executant” înseamnă statul membru care întreprinde acțiunile necesare în urma obținerii unui rezultat pozitiv;

(k) „utilizatori finali” înseamnă autoritățile competente care efectuează căutări în mod direct în CS-SIS, N.SIS sau o copie tehnică a acestora;

(l) „returnare” înseamnă returnarea astfel cum este definită la articolul 3 punctul 3 din Directiva 2008/115/CE;

(m) „interdicție de intrare” înseamnă interdicția de intrare astfel cum este definită la articolul 3 punctul 6 din Directiva 2008/115/CE;

(n) „date dactiloscopice” înseamnă datele privind amprentele digitale și amprentele palmare care, având în vedere unicitatea acestora și punctele de referință pe care le conțin, permit comparații fiabile și concludente referitoare la identitatea unei persoane;

(o) „infracțiune gravă” înseamnă infracțiunile menționate la articolul 2 alineatele (1) și (2) din Decizia-cadru 2002/584/JAI din 13 iunie 2002[68];

(p) „infracțiuni de terorism” înseamnă infracțiunile prevăzute de dreptul național menționate la articolele 1-4 din Decizia-cadru 2002/475/JAI din 13 iunie 2002[69].

Articolul 4
Arhitectura tehnică a SIS și modul de funcționare a acestuia

1. SIS este compus din următoarele elemente:

(a) un sistem central (SIS central) format din:

– o funcție de asistență tehnică („CS-CIS”) ce conține o bază de date, „baza de date din SIS”;

– o interfață națională uniformă (NI-SIS);

(b) un sistem național (N.SIS) în fiecare stat membru, care constă în sisteme naționale de date care comunică cu SIS central. Un N.SIS conține un fișier de date (o „copie națională”) care include o copie integrală sau parțială a bazei de date din SIS, precum și o copie de rezervă a N.SIS. În vederea asigurării disponibilității neîntrerupte pentru utilizatorii finali, N.SIS și copia sa de rezervă pot fi folosite simultan;

(c) o infrastructură de comunicare între CS-SIS și NI-SIS (infrastructura de comunicare) ce furnizează o rețea virtuală criptată destinată datelor din SIS și schimbului de date între birourile SIRENE, astfel cum se menționează la articolul 7 alineatul (2).

2. Datele din SIS se introduc, se actualizează, se șterg și se consultă prin efectuarea de căutări prin intermediul diverselor N.SIS. O copie națională parțială sau integrală este disponibilă pentru efectuarea de căutări automate pe teritoriul fiecărui stat membru care utilizează o astfel de copie. Copia națională parțială conține cel puțin datele enumerate la articolul 20 alineatul (2) literele (a)-(v) din prezentul regulament. Nu este posibil să se efectueze căutări în fișierele de date din sistemul N.SIS al altor state membre.

3. CS-SIS îndeplinește funcțiile de supraveghere tehnică și de administrare și are o copie de rezervă care poate să asigure toate funcționalitățile CS-SIS principal, în cazul în care acesta încetează să funcționeze. CS-SIS și copia de rezervă a CS-SIS sunt amplasate în două sedii tehnice ale Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate,

[68] Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (JO L 190, 18.7.2002, p. 1).

[69] Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO L 164, 22.6.2002, p. 3).

Securitate și Justiție, instituită prin Regulamentul (UE) nr. 1077/2011[70] („agenția”). CS-SIS sau copia de rezervă a CS-SIS poate conține o copie suplimentară a bazei de date din SIS și acestea pot fi utilizate simultan în modalitatea de funcționare activă, cu condiția ca fiecare dintre acestea să fie în măsură să prelucreze toate operațiunile referitoare la semnalările din SIS.

4. CS-SIS furnizează serviciile necesare pentru introducerea și prelucrarea datelor din SIS, inclusiv căutările în baza de date din SIS. CS-SIS asigură:

(a) actualizarea online a copiilor naționale;

(b) sincronizarea și coerența dintre copiile naționale și baza de date din SIS;

(c) operațiunile de inițializare și de restabilire a copiilor naționale;

(d) disponibilitatea neîntreruptă.

Articolul 5
Costuri

1. Costurile aferente funcționării, întreținerii și dezvoltării în continuare a SIS central și a infrastructurii de comunicare se suportă din bugetul general al Uniunii Europene.

2. Aceste costuri includ lucrările care vizează CS-SIS și asigură furnizarea serviciilor menționate la articolul 4 alineatul (4).

3. Costurile aferente înființării, funcționării, întreținerii și dezvoltării în continuare a fiecărui N.SIS sunt suportate de statul membru în cauză.

CAPITOLUL II

RESPONSABILITĂȚILE STATELOR MEMBRE

Articolul 6
Sistemele naționale

Fiecare stat membru este responsabil cu înființarea, funcționarea, întreținerea și dezvoltarea în continuare a sistemului său N.SIS și cu conectarea acestuia la NI-SIS.

Fiecare stat membru este responsabil să asigure funcționarea continuă a N.SIS, conectarea acestuia cu NI-SIS și disponibilitatea neîntreruptă a datelor din SIS pentru utilizatorii finali.

Articolul 7
Oficiul N.SIS și biroul SIRENE

1. Fiecare stat membru desemnează o autoritate (oficiul N.SIS) care deține responsabilitatea principală pentru sistemul său N.SIS.

Autoritatea respectivă este responsabilă cu buna funcționare și securitatea N.SIS, asigură accesul autorităților competente la SIS și ia măsurile necesare pentru a garanta respectarea dispozițiilor prezentului regulament. Aceasta este responsabilă să

[70] Instituită prin Regulamentul (UE) nr. 1077/2011 al Parlamentului European și al Consiliului din 25 octombrie 2011 de instituire a Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (JO L 286, 1.11.2011, p. 1).

asigure faptul că toate funcționalitățile SIS sunt puse în mod corespunzător la dispoziția utilizatorilor finali.

Fiecare stat membru transmite semnalările sale prin intermediul oficiului său N.SIS.

2. Fiecare stat membru desemnează autoritatea care trebuie să asigure schimbul și disponibilitatea tuturor informațiilor suplimentare (biroul SIRENE) în conformitate cu dispozițiile Manualului SIRENE, astfel cum se menționează la articolul 8.

Aceste birouri coordonează, de asemenea, verificarea calității informațiilor introduse în SIS. În aceste scopuri, birourile SIRENE au acces la datele prelucrate în SIS.

3. Statele membre informează agenția cu privire la oficiul lor N.SIS II și la biroul lor SIRENE. Agenția publică lista acestora, împreună cu lista menționată la articolul 36 alineatul (8).

Articolul 8
Schimbul de informații suplimentare

1. Schimbul de informații suplimentare se efectuează în conformitate cu dispozițiile Manualului SIRENE și cu ajutorul infrastructurii de comunicare. Statele membre furnizează resursele tehnice și de personal necesare pentru a se asigura disponibilitatea continuă și schimbul de informații suplimentare. În cazul în care infrastructura de comunicare nu poate fi utilizată, statele membre pot folosi pentru schimbul de informații suplimentare alte mijloace tehnice, securizate în mod corespunzător.

2. Informațiile suplimentare se utilizează numai în scopul pentru care au fost transmise în conformitate cu articolul 43, cu excepția cazului în care s-a obținut în prealabil acordul statului membru semnalant.

3. Birourile SIRENE își îndeplinesc sarcinile într-un mod rapid și eficient, în special prin formularea unui răspuns la o cerere cât mai curând posibil, dar nu mai târziu de 12 ore de la primirea cererii.

4. Normele detaliate privind schimbul de informații suplimentare se adoptă prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 55 alineatul (2), sub forma unui manual intitulat „Manualul SIRENE”.

Articolul 9
Conformitatea tehnică și funcțională

1. La crearea sistemului său N.SIS, fiecare stat membru respectă standardele, protocoalele și procedurile tehnice comune stabilite pentru a se asigura compatibilitatea sistemului său N-SIS cu CS-SIS în vederea unei transmiteri prompte și eficace a datelor. Aceste standarde, protocoale și proceduri tehnice comune se stabilesc și se precizează prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 55 alineatul (2).

2. Statele membre se asigură, prin intermediul serviciilor furnizate de CS-SIS, că datele stocate în copia națională sunt identice și coerente cu baza de date din SIS, prin efectuarea actualizărilor automate menționate la articolul 4 alineatul (4), și că în urma efectuării unei căutări în copia lor națională se obține un rezultat echivalent cu cel generat de efectuarea unei căutări în baza de date din SIS. Utilizatorii finali primesc datele necesare pentru îndeplinirea sarcinilor care le revin, în special toate

datele necesare pentru identificarea persoanei vizate și pentru întreprinderea acțiunii necesare.

Articolul 10
Securitatea – statele membre

1. Fiecare stat membru adoptă, în legătură cu sistemul său N.SIS, măsurile necesare, inclusiv un plan de securitate, un plan de asigurare a continuității activității și un plan de recuperare în caz de dezastru, pentru:

(a) a proteja datele din punct de vedere fizic, inclusiv prin elaborarea de planuri de urgență pentru protecția infrastructurii critice;

(b) a împiedica accesul persoanelor neautorizate la instalațiile de prelucrare a datelor utilizate pentru prelucrarea datelor cu caracter personal (controlul accesului la instalații);

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

(d) a împiedica introducerea neautorizată de date și inspectarea, modificarea sau ștergerea neautorizată a datelor cu caracter personal stocate (controlul stocării);

(e) a împiedica utilizarea sistemelor de prelucrare automată a datelor de către persoane neautorizate cu ajutorul echipamentelor de comunicare a datelor (controlul utilizării);

(f) a se asigura că persoanele autorizate să utilizeze un sistem de prelucrare automată a datelor au acces numai la datele pentru care dețin autorizația de acces, prin utilizarea unor identități de utilizator individuale și unice și cu folosirea exclusivă a unor moduri de acces confidențiale (controlul accesului la date);

(g) a se asigura că toate autoritățile cu drept de acces la SIS sau la instalațiile de prelucrare a datelor creează profiluri care descriu funcțiile și responsabilitățile persoanelor autorizate să acceseze, să introducă, să actualizeze și să efectueze căutări în date și că pun fără întârziere aceste profiluri la dispoziția autorităților naționale de supraveghere menționate la articolul 50 alineatul (1), la cererea acestora (profilurile membrilor personalului);

(h) a se asigura că este posibil să se verifice și să se stabilească organismele cărora le pot fi transmise date cu caracter personal prin utilizarea echipamentelor de comunicare a datelor (controlul comunicării);

(i) a se asigura că ulterior este posibil să se verifice și să se stabilească ce date cu caracter personal au fost introduse în sistemele de prelucrare automată a datelor, când, de către cine și în ce scop au fost introduse datele (controlul introducerii);

(j) a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transferurilor de date cu caracter personal sau în timpul transportului suporturilor de date, în special prin utilizarea unor tehnici de criptare corespunzătoare (controlul transportului);

(k) a monitoriza eficacitatea măsurilor de securitate menționate la prezentul alineat și a lua măsurile organizaționale necesare referitoare la monitorizarea internă (auditul intern).

2. Statele membre iau măsuri echivalente celor menționate la alineatul (1) în materie de securitate în ceea ce privește prelucrarea informațiilor suplimentare și schimbul de informații suplimentare, inclusiv securizarea sediilor birourilor SIRENE.

3. Statele membre iau măsuri echivalente celor menționate la alineatul (1) în materie de securitate în ceea ce privește prelucrarea datelor din SIS de către autoritățile menționate la articolul 29.

Articolul 11
Confidențialitatea – statele membre

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 și cu informații suplimentare, 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.

Articolul 12
Păstrarea înregistrărilor la nivel național

1. Statele membre se asigură că orice accesare a datelor cu caracter personal și toate schimburile de date cu caracter personal din CS-SIS sunt înregistrate în sistemul lor N.SIS în scopul verificării legalității căutării efectuate în date, al monitorizării legalității prelucrării datelor, al automonitorizării și al asigurării funcționării corespunzătoare a N.SIS și a integrității și securității datelor.

2. Înregistrările arată, în special, istoricul semnalării, data și ora activității de prelucrare a datelor, tipul de date utilizate pentru efectuarea unei căutări, o mențiune cu privire la tipul de date transmise, denumirea autorității competente și numele persoanei responsabile cu prelucrarea datelor.

3. În cazul în care căutarea se efectuează cu ajutorul datelor dactiloscopice sau al imaginilor faciale în conformitate cu articolul 22, înregistrările arată, în special, tipul de date utilizate pentru efectuarea unei căutări, o mențiune cu privire la tipul de date transmise, denumirea autorității competente și numele persoanei responsabile cu prelucrarea datelor.

4. Înregistrările se pot utiliza numai în scopurile menționate la alineatul (1) și se șterg cel mai devreme după un an și cel mai târziu după trei ani de la creare.

5. Înregistrările se pot păstra mai mult timp dacă sunt necesare pentru proceduri de monitorizare care se află deja în curs.

6. Autoritățile naționale competente responsabile cu verificarea legalității căutărilor efectuate în date, cu monitorizarea legalității prelucrării datelor, cu automonitorizarea și cu asigurarea funcționării corespunzătoare a N.SIS și a integrității și securității datelor au acces, în limitele competenței lor și la cerere, la aceste înregistrări în scopul îndeplinirii atribuțiilor care le revin.

Articolul 13
Automonitorizarea

Statele membre se asigură că fiecare autoritate care are drept de acces la datele din SIS ia măsurile necesare pentru a respecta prezentul regulament și cooperează, dacă este necesar, cu autoritatea națională de supraveghere.

Articolul 14
Formarea personalului

Înainte de a fi autorizat să prelucreze datele stocate în SIS și periodic după acordarea accesului la datele din SIS, personalul autorităților care au drept de acces la SIS beneficiază de o formare corespunzătoare privind securitatea datelor, normele de protecție a datelor și procedurile referitoare la prelucrarea datelor, astfel cum se prevede în Manualul SIRENE. Personalul este informat cu privire la toate infracțiunile și sancțiunile relevante.

CAPITOLUL III

RESPONSABILITĂȚILE AGENȚIEI

Articolul 15
Gestionarea operațională

1. Agenția este responsabilă cu gestionarea operațională a SIS central. Agenția se asigură, în cooperare cu statele membre și cu ajutorul unei analize cost-beneficiu, că pentru SIS central se utilizează în permanență cea mai bună tehnologie disponibilă.
2. Agenția este, de asemenea, responsabilă cu următoarele sarcini legate de infrastructura de comunicare:
   (a) supravegherea;
   (b) securitatea;
   (c) coordonarea relațiilor dintre statele membre și furnizor.
3. Comisia este responsabilă cu toate celelalte sarcini legate de infrastructura de comunicare, în special:
   (a) sarcinile aferente execuției bugetare;
   (b) achiziții și reînnoire;
   (c) aspecte contractuale.
4. Agenția este, de asemenea, responsabilă cu următoarele sarcini legate de birourile SIRENE și comunicarea dintre birourile SIRENE:
   (a) coordonarea și gestionarea testării;
   (b) întreținerea și actualizarea specificațiilor tehnice pentru schimbul de informații suplimentare dintre birourile SIRENE și infrastructura de comunicare și gestionarea impactului modificărilor tehnice în cazul în care acestea afectează atât SIS, cât și schimbul de informații suplimentare dintre birourile SIRENE.

5. Agenția dezvoltă și menține un mecanism și proceduri pentru verificarea calității datelor în CS-SIS și furnizează rapoarte periodice statelor membre. Agenția furnizează Comisiei un raport periodic care abordează problemele întâmpinate și statele membre afectate. Acest mecanism, precum și procedurile și interpretarea respectării standardelor privind calitatea datelor se stabilesc și se precizează prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 55 alineatul (2).

6. Gestionarea operațională a SIS central constă în toate sarcinile necesare menținerii SIS central în funcțiune 24 de ore pe zi, șapte zile pe săptămână în conformitate cu prezentul regulament, în special activitatea de întreținere și dezvoltările tehnice necesare pentru buna funcționare a sistemului. Aceste sarcini includ, de asemenea, activitățile de testare care asigură faptul că SIS central și sistemele naționale funcționează în conformitate cu cerințele tehnice și funcționale, astfel cum se prevede la articolul 9 din prezentul regulament.

Articolul 16
Securitatea

1. Agenția adoptă măsurile necesare, inclusiv un plan de securitate, un plan de asigurare a continuității activității și un plan de recuperare în caz de dezastru pentru SIS central și infrastructura de comunicare în scopul de:

   (a) a proteja datele din punct de vedere fizic, inclusiv prin elaborarea de planuri de urgență pentru protecția infrastructurii critice;

   (b) a împiedica accesul persoanelor neautorizate la instalațiile de prelucrare a datelor utilizate pentru prelucrarea datelor cu caracter personal (controlul accesului la instalații);

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

   (d) a împiedica introducerea neautorizată de date și inspectarea, modificarea sau ștergerea neautorizată a datelor cu caracter personal stocate (controlul stocării);

   (e) a împiedica utilizarea sistemelor de prelucrare automată a datelor de către persoane neautorizate cu ajutorul echipamentelor de comunicare a datelor (controlul utilizării);

   (f) a se asigura că persoanele autorizate să utilizeze un sistem de prelucrare automată a datelor au acces numai la datele pentru care dețin autorizația de acces, prin utilizarea unor identități de utilizator individuale și unice și cu folosirea exclusivă a unor moduri de acces confidențiale (controlul accesului la date);

   (g) a crea profiluri care descriu funcțiile și responsabilitățile persoanelor care sunt autorizate să acceseze datele sau instalațiile de prelucrare a datelor și de a pune fără întârziere aceste profiluri la dispoziția Autorității Europene pentru Protecția Datelor menționate la articolul 51, la cererea acesteia (profilurile membrilor personalului);

   (h) a se asigura că este posibil să se verifice și să se stabilească organismele cărora le pot fi transmise date cu caracter personal prin utilizarea echipamentelor de comunicare a datelor (controlul comunicării);

(i) a se asigura că ulterior este posibil să se verifice și să se stabilească ce date cu caracter personal au fost introduse în sistemele de prelucrare automată a datelor, când și de către cine au fost introduse datele (controlul introducerii);

(j) a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transferurilor de date cu caracter personal sau în timpul transportului suporturilor de date, în special prin utilizarea unor tehnici de criptare corespunzătoare (controlul transportului);

(k) a monitoriza eficacitatea măsurilor de securitate prevăzute la prezentul alineat și a lua măsurile organizaționale necesare referitoare la monitorizarea internă, astfel încât să se asigure conformitatea cu prezentul regulament (audit intern).

2. Agenția ia măsuri echivalente celor menționate la alineatul (1) în materie de securitate în ceea ce privește prelucrarea informațiilor suplimentare și schimbul de informații suplimentare prin intermediul infrastructurii de comunicare.

Articolul 17
Confidențialitatea – agenția

1. Fără a aduce atingere articolului 17 din Statutul funcționarilor Uniunii Europene și Regimul aplicabil celorlalți agenți ai Uniunii Europene, agenția 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 articolul 11 din prezentul regulament. 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.

2. Agenția ia măsuri echivalente celor menționate la alineatul (1) în materie de confidențialitate în ceea ce privește schimbul de informații suplimentare prin intermediul infrastructurii de comunicare.

Articolul 18
Păstrarea înregistrărilor la nivel central

1. Agenția se asigură că orice accesare a datelor cu caracter personal și toate schimburile de date cu caracter personal din CS-SIS sunt înregistrate în scopurile menționate la articolul 12 alineatul (1).

2. Înregistrările arată, în special, istoricul semnalărilor, data și ora la care au fost transmise datele, tipul de date utilizate pentru efectuarea de căutări, mențiunea cu privire la tipul de date transmise și denumirea autorității competente responsabile cu prelucrarea datelor.

3. În cazul în care căutarea se efectuează cu ajutorul datelor dactiloscopice sau al imaginilor faciale în conformitate cu articolele 22 și 28, înregistrările arată, în special, tipul de date utilizate pentru efectuarea unei căutări, o mențiune cu privire la tipul de date transmise, denumirea autorității competente și numele persoanei responsabile cu prelucrarea datelor.

4. Înregistrările se pot utiliza numai în scopurile menționate la alineatul (1) și se șterg cel mai devreme după un an și cel mai târziu după trei ani de la creare. Înregistrările care includ istoricul semnalărilor se șterg în termen de unu până la trei ani de la ștergerea semnalărilor.

5. Înregistrările se pot păstra mai mult timp dacă sunt necesare pentru proceduri de monitorizare care se află deja în curs.

6. Autoritățile competente responsabile cu verificarea legalității unei căutări efectuate în date, monitorizarea legalității prelucrării datelor, automonitorizarea și asigurarea funcționării corespunzătoare a CS-SIS și a integrității și securității datelor au acces, în limitele competenței lor și la cerere, la aceste înregistrări în scopul îndeplinirii sarcinilor care le revin.

CAPITOLUL IV

INFORMAREA PUBLICULUI

Articolul 19
Campanii de informare privind SIS

Comisia, în cooperare cu autoritățile naționale de supraveghere și cu Autoritatea Europeană pentru Protecția Datelor, efectuează periodic campanii de informare a publicului privind obiectivele SIS, datele stocate, autoritățile care au acces la SIS și drepturile persoanelor vizate. Statele membre, în cooperare cu propriile autorități naționale de supraveghere, elaborează și pun în aplicare politicile necesare de informare generală a cetățenilor lor cu privire la SIS.

CAPITOLUL V

SEMNALĂRILE EMISE CU PRIVIRE LA RESORTISANȚII ȚĂRILOR TERȚE ÎN SCOPUL REFUZĂRII INTRĂRII ȘI A ȘEDERII

Articolul 20
Categoriile de date

1. Fără a aduce atingere articolului 8 alineatul (1) sau dispozițiilor prezentului regulament care prevăd stocarea de date suplimentare, SIS conține doar categoriile de date care sunt furnizate de fiecare stat membru și care sunt necesare pentru scopurile prevăzute la articolul 24.

2. Informațiile privind persoanele care fac obiectul unei semnalări conțin doar următoarele date:

   (a) numele;

   (b) prenumele;

   (c) numele la naștere;

   (d) numele folosite anterior și numele de împrumut;

   (e) orice caracteristică fizică specifică, obiectivă și inalterabilă;

   (f) locul nașterii;

   (g) data nașterii;

(h) sexul;

(i) cetățenia/cetățeniile;

(j) dacă persoana vizată este înarmată, este violentă, a evadat sau este implicată într-o activitate de tipul celor menționate la articolele 1, 2, 3 și 4 din Decizia-cadru 2002/475/JAI a Consiliului privind combaterea terorismului;

(k) motivul semnalării;

(l) autoritatea care emite semnalarea;

(m) o trimitere la decizia care a generat semnalarea;

(n) acțiunea care trebuie întreprinsă;

(o) conexiunea (conexiunile) cu alte semnalări emise în SIS în temeiul articolului 38;

(p) dacă persoana vizată este membru de familie al unui cetățean al UE sau o altă persoană care beneficiază de drepturi de liberă circulație, astfel cum se menționează la articolul 25;

(q) dacă decizia privind refuzul intrării se bazează pe:

– o condamnare anterioară, astfel cum se menționează la articolul 24 alineatul (2) litera (a);

– o amenințare gravă la adresa securității, astfel cum se menționează la articolul 24 alineatul (2) litera (b);

– o interdicție de intrare, astfel cum se menționează la articolul 24 alineatul (3) sau

– o măsură restrictivă, astfel cum se menționează la articolul 27;

(r) tipul de infracțiune [pentru semnalările emise în temeiul articolului 24 alineatul (2) din prezentul regulament];

(s) categoria documentului de identificare al persoanei;

(t) țara care a eliberat documentul de identificare al persoanei;

(u) numărul (numerele) documentului de identificare al persoanei;

(v) data eliberării documentului de identificare al persoanei;

(w) fotografii și imagini faciale;

(x) date dactiloscopice;

(y) o copie color a documentului de identitate.

3. Normele tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatul (2) și efectuarea de căutări în acestea se stabilesc și se precizează prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 55 alineatul (2).

4. Normele tehnice necesare pentru efectuarea de căutări în datele menționate la alineatul (2) se stabilesc și se precizează în conformitate cu procedura de examinare menționată la articolul 55 alineatul (2). Aceste norme tehnice sunt similare în cazul căutărilor efectuate în CS-SIS, în copiile naționale și în copiile tehnice, astfel cum se menționează la articolul 36, și se bazează pe standarde comune stabilite și precizate

prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 55 alineatul (2).

Articolul 21
Proporționalitatea

1. Înainte de a emite o semnalare și atunci când prelungesc perioada de valabilitate a unei semnalări, statele membre stabilesc dacă respectivul caz este suficient de adecvat, relevant și important pentru a se justifica introducerea unei semnalări în SIS.

2. Pentru a aplica articolul 24 alineatul (2), statele membre trebuie să creeze în toate circumstanțele o astfel de semnalare privind resortisanții țărilor terțe dacă infracțiunea intră sub incidența articolelor 1-4 din Decizia-cadru 2002/475/JAI a Consiliului privind combaterea terorismului[71].

Articolul 22
Norme specifice privind introducerea fotografiilor, a imaginilor faciale și a datelor dactiloscopice

1. Datele menționate la articolul 20 alineatul (2) literele (w) și (x) se introduc în SIS doar în urma unei verificări a calității pentru a se asigura îndeplinirea unui standard minim de calitate a datelor.

2. Pentru stocarea datelor menționate la alineatul (1) se stabilesc standarde de calitate. Specificațiile acestor standarde se stabilesc prin intermediul unor măsuri de punere în aplicare și se actualizează în conformitate cu procedura de examinare menționată la articolul 55 alineatul (2).

Articolul 23
Cerințe privind introducerea unei semnalări

1. O semnalare nu poate fi introdusă fără datele menționate la articolul 20 alineatul (2) literele (a), (g), (k), (m), (n) și (q). În cazul în care o semnalare se bazează pe o decizie luată în temeiul articolului 24 alineatul (2), se introduc, de asemenea, datele menționate la articolul 20 alineatul (2) litera (r).

2. În cazul în care sunt disponibile, se introduc, de asemenea, toate celelalte date menționate la articolul 20 alineatul (2).

Articolul 24
Condiții de emitere a semnalărilor privind refuzul intrării și al șederii

1. Datele privind resortisanții țărilor terțe care fac obiectul unei semnalări în scopul refuzării intrării și a șederii se introduc în SIS pe baza unei semnalări naționale care este rezultatul unei decizii luate de autoritățile administrative sau judiciare competente în conformitate cu regulamentul de procedură prevăzut de dreptul național, pe baza unei evaluări individuale. Căile de atac împotriva acestor decizii se exercită în conformitate cu dreptul național.

[71] Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO L 164, 22.6.2002, p. 3).

2. Se introduce o semnalare atunci când decizia menționată la alineatul (1) se bazează pe o amenințare la adresa ordinii publice sau a siguranței publice ori la adresa securității naționale pe care o poate constitui prezența resortisantului țării terțe în cauză pe teritoriul unui stat membru. Această situație apare în special în cazul:

   (a) unui resortisant al unei țări terțe care a fost condamnat într-un stat membru pentru o infracțiune care se pedepsește cu privare de libertate de cel puțin un an;

   (b) unui resortisant al unei țări terțe despre care există motive întemeiate să se creadă că a comis o infracțiune gravă sau despre care există indicii clare că intenționează să comită o astfel de infracțiune pe teritoriul unui stat membru.

3. Se introduce o semnalare atunci când decizia menționată la alineatul (1) este o interdicție de intrare emisă în conformitate cu proceduri care respectă Directiva 2008/115/CE. Statul membru semnalant se asigură că semnalarea produce efecte în SIS la punctul de returnare a resortisantului țării terțe în cauză. Confirmarea returnării se comunică statului membru semnalant în conformitate cu articolul 6 din Regulamentul (UE) 2018/xxx [Regulamentul privind returnarea].

Articolul 25
Condiții de introducere a semnalărilor privind resortisanții țărilor terțe care beneficiază de dreptul la liberă circulație pe teritoriul Uniunii

1. O semnalare privind un resortisant al unei țări terțe care beneficiază de dreptul la liberă circulație pe teritoriul Uniunii, în sensul Directivei 2004/38/CE a Parlamentului European și a Consiliului[72], se introduce în conformitate cu măsurile adoptate pentru transpunerea directivei menționate.

2. În cazul obținerii unui rezultat pozitiv referitor la o semnalare prevăzută la articolul 24 cu privire la un resortisant al unei țări terțe care beneficiază de dreptul la liberă circulație pe teritoriul Uniunii, statul membru care execută semnalarea consultă imediat statul membru semnalant, prin intermediul schimbului de informații suplimentare, pentru a stabili fără întârziere acțiunea care trebuie întreprinsă.

Articolul 26
Procedura de consultare

1. În cazul în care un stat membru are în vedere să acorde un permis de ședere sau o altă autorizație care conferă un drept de ședere unui resortisant al unei țări terțe care face obiectul unei semnalări privind refuzul intrării și al șederii introduse de un alt stat membru, acesta consultă mai întâi, prin intermediul schimbului de informații suplimentare, statul membru semnalant și ține seama de interesele respectivului stat membru. Statul membru semnalant transmite un răspuns clar în termen de șapte zile. Dacă statul membru care are în vedere să acorde un permis sau o altă autorizație care conferă un drept de ședere decide să acorde respectivul permis sau respectiva autorizație, semnalarea privind refuzul intrării și al șederii trebuie ștearsă.

2. În cazul în care un stat membru are în vedere să introducă o semnalare privind refuzul intrării și al șederii având ca obiect un resortisant al unei țări terțe care este titularul unui permis de ședere valabil sau al unei alte autorizații care conferă un

[72] JO L 158, 30.4.2004, p. 77.

drept de ședere, eliberat(ă) de un alt stat membru, acesta consultă mai întâi, prin intermediul schimbului de informații suplimentare, statul membru care a eliberat permisul și ține seama de interesele respectivului stat membru. Statul membru care a eliberat permisul transmite un răspuns clar în termen de șapte zile. Dacă statul membru care a eliberat permisul decide să îl mențină, nu se introduce semnalarea privind refuzul intrării și al șederii.

3. În cazul obținerii unui rezultat pozitiv referitor la o semnalare privind refuzul intrării și al șederii având ca obiect un resortisant al unei țări terțe care este titularul unui permis de ședere valabil sau al unei alte autorizații care conferă un drept de ședere, statul membru executant consultă imediat, prin intermediul schimbului de informații suplimentare, statul membru care a eliberat permisul de ședere și, respectiv, statul membru care a introdus semnalarea pentru a stabili dacă acțiunea poate fi întreprinsă. În cazul în care se decide să se mențină permisul de ședere, semnalarea trebuie ștearsă.

4. Statele membre furnizează anual agenției statistici privind consultările efectuate în conformitate cu alineatele (1)-(3).

Articolul 27

Condițiile de emitere a semnalărilor privind resortisanții țărilor terțe care fac obiectul unor măsuri restrictive

1. Semnalările privind resortisanții țărilor terțe care fac obiectul unei măsuri restrictive menite să nu le permită intrarea pe teritoriul statelor membre sau tranzitarea acestui teritoriu și luate în conformitate cu acte juridice adoptate de Consiliu, inclusiv al măsurilor de punere în aplicare a unei interdicții de călătorie emise de Consiliul de Securitate al Organizației Națiunilor Unite, se introduc în SIS, în măsura în care sunt respectate cerințele privind calitatea datelor, în scopul refuzării intrării și a șederii.

2. Statul membru responsabil cu introducerea, actualizarea și ștergerea acestor semnalări în numele tuturor statelor membre este desemnat la momentul adoptării măsurii relevante luate în conformitate cu articolul 29 din Tratatul privind Uniunea Europeană. Procedura de desemnare a statului membru responsabil se stabilește și se precizează prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 55 alineatul (2).

CAPITOLUL VI

EFECTUAREA DE CĂUTĂRI CU AJUTORUL DATELOR BIOMETRICE

Articolul 28

Norme specifice privind verificarea sau efectuarea de căutări cu ajutorul fotografiilor, al imaginilor faciale și al datelor dactiloscopice

1. Fotografiile, imaginile faciale și datele dactiloscopice se extrag din SIS pentru a verifica identitatea unei persoane care a fost localizată în urma unei căutări alfanumerice efectuate în SIS.

2. Datele dactiloscopice se pot utiliza, de asemenea, pentru identificarea unei persoane. Datele dactiloscopice stocate în SIS se utilizează în scopul identificării dacă identitatea persoanei nu poate fi stabilită prin alte mijloace.

3. În datele dactiloscopice stocate în SIS în legătură cu semnalări emise în temeiul articolului 24 se pot efectua, de asemenea, căutări cu ajutorul unor seturi complete sau incomplete de amprente digitale sau de amprente palmare descoperite la locurile unor infracțiuni în curs de investigare și în cazul în care se poate stabili cu un grad ridicat de probabilitate că acestea aparțin autorului infracțiunii, cu condiția ca autoritățile competente să nu fie în măsură să stabilească identitatea persoanei în cauză prin utilizarea niciunei alte baze de date naționale, europene sau internaționale.

4. De îndată ce acest lucru devine posibil din punct de vedere tehnic, asigurând totodată un nivel ridicat de fiabilitate a identificării, se pot utiliza fotografii și imagini faciale pentru identificarea unei persoane. Identificarea pe baza fotografiilor sau a imaginilor faciale se utilizează doar în contextul punctelor obișnuite de trecere a frontierei în cazul în care se utilizează sistemele de control self-service și sistemele de control automat la frontieră.

CAPITOLUL VII

DREPTUL DE ACCES LA SEMNALĂRI ȘI PĂSTRAREA ACESTORA

Articolul 29
Autoritățile care au drept de acces la semnalări

1. Accesul la datele introduse în SIS și dreptul de a efectua căutări în aceste date în mod direct sau într-o copie a datelor din SIS sunt rezervate autorităților responsabile cu identificarea resortisanților țărilor terțe în scopul:

   (a) controlul la frontiere, în conformitate cu 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);

   (b) verificările polițienești și vamale efectuate pe teritoriul statului membru în cauză și coordonarea acestor verificări de către autoritățile desemnate;

   (c) alte activități de asigurare a respectării legii efectuate pentru prevenirea, depistarea și investigarea infracțiunilor pe teritoriul statului membru în cauză;

   (d) examinarea condițiilor și luarea deciziilor privind intrarea și șederea resortisanților țărilor terțe pe teritoriul statelor membre, inclusiv privind permisele de ședere și vizele de lungă ședere, și privind returnarea resortisanților țărilor terțe.

   (e) examinării cererilor de viză și luării deciziilor privind cererile respective, inclusiv privind eventuala anulare, revocare sau prelungire a vizelor, în conformitate cu Regulamentul (UE) nr. 810/2009 al Parlamentului European și al Consiliului[73].

2. În sensul articolului 24 alineatele (2) și (3) și al articolului 27, dreptul de acces la datele introduse în SIS și dreptul de a efectua căutări în mod direct în aceste date pot fi exercitate și de către autoritățile judiciare naționale, inclusiv cele responsabile cu inițierea urmăririi penale în cadrul acțiunilor penale și cu anchetele judiciare

[73] Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului din 13 iulie 2009 privind instituirea unui Cod comunitar de vize (Codul de vize) (JO L 243, 15.9.2009, p. 1).

anterioare punerii sub acuzare, în îndeplinirea sarcinilor care le revin, astfel cum se prevede în legislația națională, precum și de către autoritățile lor coordonatoare.

3. Dreptul de acces la datele privind documente referitoare la persoane, introduse în conformitate cu articolul 38 alineatul (2) literele (j) și (k) din Regulamentul (UE) 2018/xxx [cooperarea polițienească și cooperarea judiciară în materie penală], și dreptul de a efectua căutări în aceste date pot fi exercitate, de asemenea, de către autoritățile menționate la alineatul (1) litera (d). Accesul acestor autorități la date este reglementat de dreptul fiecărui stat membru.

4. Autoritățile menționate la prezentul articol sunt incluse pe lista prevăzută la articolul 36 alineatul (8).

Articolul 30
Accesul Europol la datele din SIS

1. Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) are, în limitele mandatului său, dreptul de a accesa și de a efectua căutări în datele introduse în SIS.

2. Atunci când o căutare efectuată de Europol indică existența unei semnalări în SIS, Europol informează statul membru semnalant prin intermediul canalelor definite de Regulamentul (UE) 2016/794.

3. Utilizarea informațiilor obținute în urma efectuării unei căutări în SIS este condiționată de acordul statului membru în cauză. Dacă statul membru autorizează utilizarea informațiilor respective, prelucrarea acestora de către Europol intră sub incidența Regulamentului (UE) 2016/794. Europol poate comunica aceste informații țărilor terțe și organismelor terțe numai cu acordul statului membru în cauză.

4. Europol poate solicita informații suplimentare din partea statelor membre în cauză, în conformitate cu dispozițiile Regulamentului (UE) 2016/794.

5. Europol:

   (a) fără a aduce atingere alineatelor (3), (4) și (6), nu conectează părți ale SIS la niciun sistem informatic, nu transferă datele din SIS la care are acces către niciun sistem informatic pentru colectarea și prelucrarea datelor efectuate de către sau în cadrul Europol și nici nu descarcă sau copiază în alt mod vreo parte din SIS;

   (b) limitează accesul la datele introduse în SIS la personalul său autorizat în mod expres în acest sens;

   (c) adoptă și aplică măsurile prevăzute la articolele 10 și 11;

   (d) permite Autorității Europene pentru Protecția Datelor să examineze activitățile pe care le desfășoară în exercitarea dreptului său de a accesa și de a efectua căutări în datele introduse în SIS.

6. Se pot copia date numai în scopuri tehnice, cu condiția ca respectiva copiere să fie necesară pentru ca personalul Europol autorizat în mod corespunzător să efectueze o căutare directă. Dispozițiile prezentului regulament se aplică și acestor copii. Copia tehnică se utilizează pentru stocarea datelor din SIS în timp ce se efectuează căutări în aceste date. După ce s-au efectuat căutări în date, acestea trebuie șterse. Aceste utilizări nu se consideră a constitui o descărcare sau o copiere ilegală a datelor din

SIS. Europol nu copiază în alte sisteme ale sale datele semnalărilor sau datele suplimentare emise de statele membre ori datele din CS-SIS.

7. Orice copii, astfel cum se menționează la alineatul (6), care conduc la baze de date offline se pot păstra maximum 48 de ore. Această perioadă se poate prelungi în caz de urgență până la încetarea urgenței. Europol raportează Autorității Europene pentru Protecția Datelor orice astfel de prelungiri.

8. Europol poate primi și prelucra informații suplimentare privind semnalările SIS corespunzătoare, cu condiția ca normele de prelucrare a datelor menționate la alineatele (2)-(7) să fie aplicate în mod adecvat.

9. În scopul verificării legalității prelucrării datelor, al automonitorizării și al asigurării securității și integrității datelor, Europol păstrează înregistrările fiecărei accesări a SIS și ale fiecărei căutări efectuate în SIS. Aceste înregistrări și documentații nu se consideră a constitui o descărcare sau o copiere ilegală a niciunei părți din SIS.

Articolul 31

Accesul la datele din SIS al echipelor europene de poliție de frontieră și gardă de coastă, al echipelor de personal implicat în sarcini legate de returnare și al membrilor echipelor de sprijin pentru gestionarea migrației

1. În conformitate cu articolul 40 alineatul (8) din Regulamentul (UE) 2016/1624, membrii echipelor europene de poliție de frontieră și gardă de coastă sau ai echipelor de personal implicat în sarcini legate de returnare, precum și ai echipelor de sprijin pentru gestionarea migrației au dreptul, în limitele mandatului lor, de a accesa și de a efectua căutări în datele introduse în SIS.

2. Membrii echipelor europene de poliție de frontieră și gardă de coastă sau ai echipelor de personal implicat în sarcini legate de returnare, precum și ai echipelor de sprijin pentru gestionarea migrației au acces și efectuează căutări în datele introduse în SIS în conformitate cu alineatul (1) prin intermediul interfeței tehnice înființate și întreținute de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă, astfel cum se menționează la articolul 32 alineatul (2).

3. În cazul în care o căutare efectuată de un membru al echipelor europene de poliție de frontieră și gardă de coastă sau al echipelor de personal implicat în sarcini legate de returnare sau de un membru al echipelor de sprijin pentru gestionarea migrației indică existența unei semnalări în SIS, statul membru semnalant este informat cu privire la aceasta. În conformitate cu articolul 40 din Regulamentul (UE) 2016/1624, membrii echipelor pot acționa ca răspuns la o semnalare în SIS numai dacă primesc instrucțiuni de la polițiștii de frontieră sau de la membrii personalului implicați în sarcini legate de returnare ai statului membru gazdă și, ca regulă generală, în prezența acestora. Statul membru gazdă poate autoriza membrii echipelor să acționeze în numele său.

4. Fiecare accesare a datelor și fiecare căutare în acestea efectuate de un membru al echipelor europene de poliție de frontieră și gardă de coastă sau al echipelor de personal implicat în sarcini legate de returnare sau de un membru al echipelor de sprijin pentru gestionarea migrației se înregistrează în conformitate cu dispozițiile articolului 12 și fiecare utilizare de către membrul respectiv a datelor pe care le-a accesat se înregistrează.

5. Accesul la datele introduse în SIS se limitează la un singur membru al echipelor europene de poliție de frontieră și gardă de coastă sau al echipelor de personal

implicat în sarcini legate de returnare sau al echipelor de sprijin pentru gestionarea migrației și nu se extinde la niciun alt membru al echipei.

6. Se adoptă și se aplică măsuri de asigurare a securității și a confidențialității, astfel cum se prevede la articolele 10 și 11.

Articolul 32

Accesul la SIS al Agenției Europene pentru Poliția de Frontieră și Garda de Coastă

1. Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă are dreptul de a accesa și de a efectua căutări în datele introduse în SIS, în conformitate cu articolele 24 și 27, în scopul de a analiza amenințările susceptibile să afecteze funcționarea sau securitatea frontierelor externe.

2. În sensul articolului 31 alineatul (2) și al prezentului articol alineatul (1), Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă creează și întreține o interfață tehnică care permite conectarea directă la SIS central.

3. În cazul în care o căutare efectuată de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă indică existența unei semnalări în SIS, aceasta informează statul membru semnalant.

4. Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă are dreptul de a accesa și de a verifica datele introduse în SIS, în conformitate cu articolele 24 și 27, în scopul de a-și îndeplini sarcinile care i-au fost atribuite de Regulamentul de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS).

5. În cazul în care o verificare efectuată de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă în sensul alineatului (2) indică existența unei semnalări în SIS, se aplică procedura prevăzută la articolul 22 din Regulamentul de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS).

6. Nicio dispoziție a prezentului articol nu trebuie interpretată ca aducând atingere dispozițiilor Regulamentului (UE) 2016/1624 privind protecția datelor și răspunderea pentru orice prelucrare neautorizată sau incorectă a acestor date de către Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă.

7. Fiecare accesare a datelor și fiecare căutare în acestea efectuate de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă se înregistrează în conformitate cu dispozițiile articolului 12 și fiecare utilizare de către Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă a datelor pe care le-a accesat se înregistrează.

8. Cu excepția cazurilor în care este necesar pentru îndeplinirea sarcinilor în scopul aplicării Regulamentului de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS), nicio parte a SIS nu se conectează la un sistem informatic pentru colectarea și prelucrarea datelor efectuate de către Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă sau în cadrul acesteia și nici nu se transferă către un astfel de sistem datele din SIS la care are acces Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă. Nicio parte a SIS nu se descarcă. Înregistrarea accesului și a căutărilor nu se consideră a constitui o descărcare ilegală sau o copiere ilegală a datelor din SIS.

9. Se adoptă și se aplică măsuri de asigurare a securității și a confidențialității, astfel cum se prevede la articolele 10 și 11.

Articolul 33
Domeniul de aplicare al accesului

Utilizatorii finali, inclusiv Europol și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă, pot accesa doar datele care le sunt necesare în scopul îndeplinirii sarcinilor care le revin.

Articolul 34
Perioada de păstrare a semnalărilor

1. Semnalările introduse în SIS în temeiul prezentului regulament se păstrează numai pe durata perioadei necesare îndeplinirii scopurilor pentru care au fost introduse.

2. Un stat membru care emite o semnalare reexaminează, în termen de cinci ani de la introducerea acesteia în SIS, nevoia de a o păstra.

3. Fiecare stat membru stabilește, după caz, perioade de reexaminare mai scurte, în conformitate cu dreptul său național.

4. În cazurile în care devine clar pentru personalul biroului SIRENE, care este responsabil de coordonarea și verificarea calității datelor, că o semnalare privind o persoană și-a atins scopul și ar trebui să fie ștearsă din SIS, personalul notifică acest lucru autorității care a creat semnalarea. Autoritatea are la dispoziție 30 de zile calendaristice de la data primirii notificării pentru a indica faptul că semnalarea a fost ștearsă sau va fi ștearsă ori pentru a motiva păstrarea semnalării. Dacă perioada de 30 de zile expiră fără un astfel de răspuns, semnalarea trebuie ștearsă de personalul biroului SIRENE. Birourile SIRENE raportează autorității lor naționale de supraveghere orice probleme recurente în acest domeniu.

5. În perioada de reexaminare, în urma unei evaluări individuale cuprinzătoare care se înregistrează, statul membru care a emis semnalarea poate decide să mențină semnalarea mai mult timp, dacă acest lucru se dovedește necesar pentru scopul în care a fost emisă. În acest caz, alineatul (2) se aplică, de asemenea, prelungirii termenului de păstrare. Orice prelungire a termenului de păstrare a unei semnalări se comunică CS-SIS.

6. Semnalările trebuie șterse în mod automat după expirarea perioadei de reexaminare menționate la alineatul (2), cu excepția cazurilor în care statul membru care a emis semnalarea a informat CS-SIS cu privire la prelungirea termenului de păstrare a semnalării în temeiul alineatului (5). CS-SIS informează în mod automat statele membre cu privire la ștergerea programată a datelor din sistem, cu patru luni în avans.

7. Statele membre întocmesc statistici privind numărul semnalărilor a căror perioadă de păstrare a fost prelungită în conformitate cu alineatul (5).

Articolul 35
Ștergerea semnalărilor

1. Semnalările privind refuzul intrării și al șederii în temeiul articolului 24 trebuie șterse atunci când decizia care a stat la baza acestora a fost retrasă de autoritatea competentă, dacă este cazul în urma procedurii de consultare menționate la articolul 26.

2. Semnalările privind resortisanții țărilor terțe care fac obiectul unei măsuri restrictive, astfel cum se menționează la articolul 27, trebuie șterse atunci când măsura de punere în aplicare a interdicției de călătorie a încetat sau a fost suspendată ori anulată.

3. Semnalările privind o persoană care a dobândit cetățenia oricărui stat ai cărui resortisanți beneficiază de dreptul la liberă circulație pe teritoriul Uniunii trebuie șterse de îndată ce statul membru semnalant ia cunoștință sau este informat în temeiul articolului 38 despre faptul că persoana în cauză a dobândit această cetățenie.

CAPITOLUL VIII

NORME GENERALE DE PRELUCRARE A DATELOR

Articolul 36
Prelucrarea datelor din SIS

1. Statele membre pot prelucra datele menționate la articolul 20 în scopul refuzării intrării și a șederii pe teritoriile lor.

2. Datele se pot copia doar în scopuri tehnice, cu condiția ca această copiere să fie necesară pentru ca autoritățile menționate la articolul 29 să poată efectua o căutare directă. Dispozițiile prezentului regulament se aplică și acestor copii. Un stat membru nu copiază datele semnalărilor sau datele suplimentare introduse de un alt stat membru din sistemul său N.SIS sau din CS-SIS în alte fișiere de date naționale.

3. Copiile tehnice, astfel cum se menționează la alineatul (2), care conduc la baze de date offline se pot păstra maximum 48 de ore. Această perioadă se poate prelungi în caz de urgență până la încetarea urgenței.

   Fără a aduce atingere primului paragraf, sunt interzise copiile tehnice care conduc la baze de date offline ce urmează să fie utilizate de autoritățile responsabile cu eliberarea vizelor, cu excepția copiilor făcute pentru a fi folosite doar într-o situație de urgență în urma indisponibilității rețelei timp de peste 24 de ore.

   Statele membre țin un inventar actualizat al acestor copii, îl pun la dispoziția autorității lor naționale de supraveghere și se asigură că dispozițiile prezentului regulament, în special cele ale articolului 10, se aplică în cazul acestor copii.

4. Accesul la date este autorizat numai în limitele competenței autorităților naționale menționate la articolul 29 și numai pentru personalul autorizat în mod corespunzător.

5. Orice prelucrare a informațiilor din SIS în alte scopuri decât cele pentru care au fost introduse în SIS trebuie să fie aibă legătură cu un caz specific și să fie justificată de necesitatea de a preveni o amenințare gravă iminentă la adresa ordinii publice și a siguranței publice, de motive întemeiate de securitate națională sau în scopul prevenirii unei infracțiuni grave. În acest scop, trebuie să se obțină o autorizare prealabilă din partea statului membru care a emis semnalarea.

6. Datele privind documentele referitoare la persoane, introduse în temeiul articolului 38 alineatul (2) literele (j) și (k) din Regulamentul (UE) 2018/xxx, se pot utiliza de autoritățile menționate la articolul 29 alineatul (1) litera (d) în conformitate cu legislația fiecărui stat membru.

7. Orice utilizare a datelor care contravine alineatelor (1)-(6) se consideră a fi utilizare abuzivă în temeiul dreptului național al fiecărui stat membru.

8. Fiecare stat membru trimite agenției o listă a autorităților sale competente care sunt autorizate să efectueze în mod direct căutări în datele din SIS în temeiul prezentului regulament, precum și orice modificări aduse acestei liste. Lista specifică, pentru fiecare autoritate, datele în care aceasta poate efectua căutări și în ce scopuri. Agenția asigură publicarea anuală a listei în *Jurnalul Oficial al Uniunii Europene*.

9. În măsura în care dreptul Uniunii nu stabilește dispoziții specifice, dreptul fiecărui stat membru se aplică datelor introduse în sistemul său N.SIS.

Articolul 37
Datele din SIS și fișierele naționale

1. Articolul 36 alineatul (2) nu aduce atingere dreptului unui stat membru de a păstra în fișierele sale naționale date din SIS în legătură cu care s-a întreprins o acțiune pe teritoriul său. Aceste date se păstrează în fișierele naționale pentru o perioadă maximă de trei ani, cu excepția cazului în care dispoziții specifice din dreptul național prevăd o perioadă de păstrare mai îndelungată.

2. Articolul 36 alineatul (2) nu aduce atingere dreptului unui stat membru de a păstra în fișierele sale naționale datele dintr-o anumită semnalare emisă în SIS de respectivul stat membru.

Articolul 38
Informații în cazul neexecutării semnalării

Dacă o acțiune solicitată nu poate fi întreprinsă, statul membru solicitat informează imediat statul membru care a emis semnalarea.

Articolul 39
Calitatea datelor prelucrate în SIS

1. Statul membru care emite o semnalare este responsabil să asigure faptul că datele sunt exacte, actualizate și introduse în mod legal în SIS.

2. Numai statul membru care a emis semnalarea este autorizat să modifice, să completeze, să corecteze, să actualizeze sau să șteargă datele pe care le-a introdus.

3. În cazul în care un stat membru, altul decât cel care a emis semnalarea, are probe care sugerează că un element al datelor conține erori de fapt sau a fost stocat ilegal, respectivul stat membru aduce acest fapt la cunoștința statului membru semnalant, prin intermediul schimbului de informații suplimentare, cât mai curând posibil și în maximum 10 zile de la data la care a identificat probele respective. Statul membru semnalant verifică respectiva comunicare și, dacă este necesar, corectează sau șterge imediat elementul în cauză.

4. În cazul în care statele membre nu ajung la un acord în termen de două luni de la data identificării inițiale a probelor, astfel cum se descrie la alineatul (3), statul membru care nu a emis semnalarea sesizează autoritățile naționale de supraveghere competente în scopul luării unei decizii.

5. Statele membre fac schimb de informații suplimentare în cazul în care o persoană depune o plângere în care susține că nu este persoana vizată de o semnalare. În cazul în care rezultatul verificării arată că, de fapt, este vorba de două persoane diferite, reclamantul este informat cu privire la măsurile prevăzute la articolul 42.

6. În cazul în care o persoană face deja obiectul unei semnalări în SIS, statul membru care introduce o nouă semnalare ajunge la un acord cu privire la introducerea semnalării cu statul membru care a introdus prima semnalare. Se ajunge la acord pe baza schimbului de informații suplimentare.

Articolul 40
Incidente de securitate

1. Orice eveniment care are sau poate avea un impact asupra securității SIS și poate cauza daune sau pierderi datelor din SIS este considerat a fi un incident de securitate, în special în cazul în care este posibil să se fi accesat datele sau în cazul în care au fost afectate sau este posibil să fi fost afectate disponibilitatea, integritatea și confidențialitatea datelor.

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

3. Statele membre notifică incidentele de securitate Comisiei, agenției și Autorității Europene pentru Protecția Datelor. Agenția notifică incidentele de securitate Comisiei și Autorității Europene pentru Protecția Datelor.

4. Informațiile privind un incident de securitate care are sau poate să aibă un impact asupra funcționării SIS într-un stat membru sau în cadrul agenției sau asupra disponibilității, a integrității și a confidențialității datelor introduse sau trimise de alte state membre se pun la dispoziția statelor membre și se raportează în conformitate cu planul de gestionare a incidentelor furnizat de agenție.

Articolul 41
Diferențierea persoanelor care prezintă caracteristici similare

În cazul în care, la momentul introducerii unei noi semnalări, se constată că există deja în SIS o persoană cu aceleași elemente de descriere a identității, se aplică următoarea procedură:

(a) biroul SIRENE contactează autoritatea solicitantă pentru a clarifica dacă semnalarea se referă sau nu la aceeași persoană;

(b) în cazul în care verificarea încrucișată arată că persoana care face obiectul noii semnalări este într-adevăr persoana deja înregistrată în SIS, biroul SIRENE aplică procedura privind introducerea de semnalări multiple, astfel cum se menționează la articolul 39 alineatul (6). În cazul în care rezultatul verificării arată că, de fapt, sunt două persoane diferite, biroul SIRENE aprobă cererea de introducere a celei de a doua semnalări, adăugând elementele necesare pentru a se evita orice identificare eronată.

Articolul 42
Date suplimentare în scopul tratării cazurilor de uzurpare de identitate

1. În cazul în care pot apărea confuzii între o persoană care face, de fapt, obiectul unei semnalări și o persoană a cărei identitate a fost uzurpată, pentru a se evita consecințele negative ale identificării eronate, statul membru semnalant adaugă în semnalare, sub rezerva acordului explicit al respectivei persoane, date care o privesc.

2. Datele privind o persoană a cărei identitate a fost uzurpată se folosesc doar în următoarele scopuri:

(a) pentru a permite autorității competente să distingă între persoana a cărei identitate a fost uzurpată și persoana care face, de fapt, obiectul semnalării;

(b) pentru a permite persoanei a cărei identitate a fost uzurpată să își dovedească identitatea și pentru a se stabili faptul că identitatea sa a fost uzurpată.

3. În sensul prezentului articol, se pot introduce și prelucra ulterior în SIS doar următoarele date cu caracter personal:

(a) numele;

(b) prenumele;

(c) numele la naștere;

(d) numele folosite anterior și orice nume de împrumut care să fie introduse separat, dacă este posibil;

(e) orice caracteristică fizică specifică, obiectivă și inalterabilă;

(f) locul nașterii;

(g) data nașterii;

(h) sexul;

(i) imagini faciale;

(j) amprente digitale;

(k) cetățenie(i);

(l) categoria documentului de identitate al persoanei;

(m) țara care a eliberat documentul de identitate al persoanei;

(n) numărul (numerele) documentului de identitate al persoanei;

(o) data eliberării documentului de identitate al persoanei;

(p) adresa victimei;

(q) numele tatălui victimei;

(r) numele mamei victimei.

4. Normele tehnice necesare pentru introducerea și prelucrarea ulterioară a datelor menționate la alineatul (3) se stabilesc prin intermediul unor măsuri de punere în aplicare prevăzute și dezvoltate în conformitate cu procedura de examinare menționată la articolul 55 alineatul (2).

5. Datele menționate la alineatul (3) trebuie șterse în același timp cu semnalarea corespunzătoare sau mai devreme, dacă respectiva persoană solicită acest lucru.

6. Doar autoritățile care au drept de acces la semnalarea corespunzătoare pot accesa datele menționate la alineatul (3). Acestea pot accesa datele respective doar în scopul evitării unei identificări eronate.

Articolul 43
Conexiunile dintre semnalări

1. Un stat membru poate crea o conexiune între semnalările pe care le introduce în SIS. Scopul unei astfel de conexiuni este de a stabili o legătură între una sau mai multe semnalări.

2. Crearea unei conexiuni nu afectează acțiunea specifică ce trebuie întreprinsă pe baza fiecărei semnalări conexe sau perioada de păstrare a fiecăreia dintre semnalările conexe.

3. Crearea unei conexiuni nu aduce atingere drepturilor de acces prevăzute în prezentul regulament. Autoritățile care nu au drept de acces la anumite categorii de semnalări nu pot vedea conexiunea către o semnalare la care nu au acces.

4. Un stat membru creează o conexiune între semnalări doar în cazul în care acest lucru este necesar din punct de vedere operațional.

5. În cazul în care un stat membru consideră că crearea de către un alt stat membru a unei conexiuni între semnalări este incompatibilă cu dreptul său național sau cu obligațiile sale internaționale, acesta poate lua măsurile necesare pentru a se asigura că respectiva conexiune nu poate fi accesată de pe teritoriul său național sau de către autoritățile sale situate în afara teritoriului său.

6. Normele tehnice privind crearea unei conexiuni între semnalări se stabilesc și se precizează în conformitate cu procedura de examinare definită la articolul 55 alineatul (2).

Articolul 44

Scopul informațiilor suplimentare și perioada de păstrare a acestora

1. Statele membre păstrează în cadrul biroului SIRENE o trimitere la deciziile care au generat o semnalare pentru a sprijini schimbul de informații suplimentare.

2. Datele cu caracter personal din fișierele deținute de biroul SIRENE ca urmare a unui schimb de informații se păstrează numai pe perioada care este necesară în vederea realizării scopurilor pentru care au fost furnizate. În orice caz, acestea trebuie șterse în termen de maximum un an după ce semnalarea conexă a fost ștearsă din SIS.

3. Alineatul (2) nu aduce atingere dreptului unui stat membru de a păstra în fișierele naționale date referitoare la o anumită semnalare pe care a emis-o respectivul stat membru sau la o semnalare în legătură cu care s-a întreprins o acțiune pe teritoriul său. Perioada pentru care aceste date se pot păstra în respectivele fișiere este reglementată de dreptul național.

Articolul 45

Transferul datelor cu caracter personal către terți

Datele prelucrate în SIS și informațiile suplimentare conexe prevăzute în prezentul regulament nu se transferă și nici nu se pun la dispoziția țărilor terțe sau a organizațiilor internaționale.

CAPITOLUL IX

PROTECȚIA DATELOR

Articolul 46
Legislația aplicabilă

1. Regulamentul (CE) nr. 45/2001 se aplică prelucrării datelor cu caracter personal de către agenție în temeiul prezentului regulament.

2. Regulamentul 2016/679 se aplică prelucrării datelor cu caracter personal de către autoritățile menționate la articolul 29 din prezentul regulament, cu condiția să nu se aplice dispozițiile naționale de transpunere a Directivei (UE) 2016/680.

3. Pentru prelucrarea datelor de către autoritățile naționale competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor penale, inclusiv în scopul asigurării prevenirii amenințărilor la adresa siguranței publice, se aplică dispozițiile naționale de transpunere a Directivei (UE) 2016/680.

Articolul 47
Dreptul de accesare, de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal

1. Dreptul persoanelor vizate de a avea acces la datele introduse în SIS care le privesc și de rectificare sau de ștergere a acestor date se exercită în conformitate cu dreptul statului membru în care invocă acest drept.

2. În cazul în care dreptul național prevede acest lucru, autoritatea națională de supraveghere decide dacă informațiile se pot comunica și prin ce mijloace.

3. Un alt stat membru decât cel care a emis o semnalare poate comunica informații privind aceste date numai dacă îi oferă mai întâi statului membru care a emis semnalarea posibilitatea de a-și face cunoscută poziția. Acest lucru se realizează prin intermediul schimbului de informații suplimentare.

4. Un stat membru ia decizia de a nu comunica, integral sau parțial, informații persoanei vizate, în conformitate cu dreptul național, în măsura în care și atât timp cât o astfel de restricționare parțială sau integrală constituie o măsură necesară și proporțională într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice vizate, pentru:

   (a) a evita obstrucționarea cercetărilor, a investigațiilor sau a procedurilor oficiale ori juridice;

   (b) a evita afectarea prevenirii, a depistării, a investigării sau a urmăririi penale a infracțiunilor sau a executării pedepselor penale;

   (c) a proteja siguranța publică;

   (d) a proteja securitatea națională;

   (e) a proteja drepturile și libertățile celorlalți.

5. Persoana vizată este informată cât mai repede posibil și, în orice caz, în maximum 60 de zile de la data la care depune cererea de acces sau mai devreme, dacă dreptul național prevede acest lucru.

6. Persoana vizată este informată cu privire la rezultatul exercitării drepturilor sale de rectificare și ștergere cât mai repede posibil și, în orice caz, în maximum trei luni de la data la care a depus cererea de rectificare sau de ștergere ori mai devreme, dacă dreptul național prevede acest lucru.

Articolul 48
Dreptul la informare

1. Resortisanții țărilor terțe care fac obiectul unei semnalări emise în temeiul prezentului regulament sunt informați în conformitate cu articolele 10 și 11 din Directiva 95/46/CE. Această informare se efectuează în scris și este însoțită de o copie a deciziei naționale care a generat semnalarea sau o trimitere la aceasta, astfel cum se menționează la articolul 24 alineatul (1).

2. Această informare nu se efectuează:

(f) în cazul în care:

(i) datele cu caracter personal nu au fost obținute de la resortisantul țării terțe în cauză

și

(ii) furnizarea informațiilor se dovedește a fi imposibilă sau ar implica un efort disproporționat;

(g) în cazul în care resortisantul țării terțe în cauză deține deja informațiile;

(h) în cazul în care dreptul național permite derogarea de la dreptul la informare, în special pentru a garanta securitatea națională și a asigura apărarea, siguranța publică și prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor.

Articolul 49
Căi de atac

1. Orice persoană poate introduce o acțiune în fața instanțelor judecătorești sau a autorității competente în temeiul dreptului național al oricărui stat membru pentru accesarea, rectificarea sau ștergerea informațiilor sau pentru obținerea de compensații în legătură cu o semnalare care o privește.

2. Statele membre se angajează reciproc să execute deciziile definitive pronunțate de instanțele judecătorești sau de autoritățile menționate la alineatul (1) al prezentului articol, fără a aduce atingere dispozițiilor articolului 53.

3. Pentru a se obține o imagine de ansamblu coerentă asupra funcționării căilor de atac, autoritățile naționale de supraveghere sunt invitate să elaboreze un sistem statistic standard pentru raportarea anuală cu privire la:

(a) numărul de cereri de acces ale persoanelor vizate înaintate operatorului de date și numărul de cazuri în care s-a acordat acces la date;

(b) numărul de cereri de acces ale persoanelor vizate înaintate autorității naționale de supraveghere și numărul de cazuri în care s-a acordat acces la date;

(c) numărul de cereri de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal înaintate operatorului de date și numărul de cazuri în care datele au fost rectificate sau șterse;

(d) numărul de cereri de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal înaintate autorității naționale de supraveghere;

(e) numărul de cauze soluționate de o instanță judecătorească;

(f) numărul de cauze în care o instanță judecătorească s-a pronunțat în favoarea reclamantului în oricare aspect al cauzei;

(g) orice observații privind cazurile de recunoaștere reciprocă a deciziilor definitive pronunțate de instanțele judecătorești sau de autoritățile altor state membre privind semnalările create de statul membru care a emis semnalarea.

Rapoartele elaborate de autoritățile naționale de supraveghere se transmit mecanismului de cooperare stabilit la articolul 52.

Articolul 50
Supravegherea N.SIS

1. Fiecare stat membru se asigură că autoritatea (autoritățile) națională(e) de supraveghere desemnată(e) în fiecare stat membru și învestită(e) cu competențele menționate în capitolul VI din Directiva (UE) 2016/680 sau în capitolul VI din Regulamentul (UE) 2016/679 monitorizează în mod independent legalitatea prelucrării datelor cu caracter personal din SIS pe teritoriul său și transmiterea acestor date de pe teritoriul său, precum și schimbul de informații suplimentare și prelucrarea lor ulterioară.

2. Autoritatea națională de supraveghere se asigură că, cel puțin din patru în patru ani, se efectuează un audit al operațiunilor de prelucrare a datelor cu caracter personal în sistemul său N.SIS, efectuat în conformitate cu standardele internaționale de audit. Auditul fie se efectuează de autoritatea (autoritățile) națională(e) de supraveghere, fie autoritatea (autoritățile) națională(e) de supraveghere dispune (dispun) în mod direct efectuarea auditului de către un auditor independent în materie de protecție a datelor. Permanent, autoritatea națională de supraveghere păstrează controlul asupra auditorului independent și își asumă responsabilitățile acestuia.

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

Articolul 51
Supravegherea agenției

1. Autoritatea Europeană pentru Protecția Datelor se asigură că activitățile de prelucrare a datelor cu caracter personal desfășurate de agenție se efectuează în conformitate cu prezentul regulament. Îndatoririle și competențele menționate la articolele 46 și 47 din Regulamentul (CE) nr. 45/2001 se aplică în consecință.

2. Autoritatea Europeană pentru Protecția Datelor se asigură că, cel puțin din patru în patru ani, se efectuează un audit al activităților de prelucrare a datelor cu caracter

personal desfășurate de agenție, în conformitate cu standardele internaționale de audit. Raportul de audit se trimite Parlamentului European, Consiliului, agenției, Comisiei și autorităților naționale de supraveghere. Agenției i se oferă posibilitatea de a face observații înainte de adoptarea raportului.

Articolul 52
Cooperarea dintre autoritățile naționale de supraveghere și Autoritatea Europeană pentru Protecția Datelor

1. Autoritățile naționale de supraveghere și Autoritatea Europeană pentru Protecția Datelor, acționând fiecare în limitele competențelor deținute, cooperează în mod activ în cadrul responsabilităților care le revin și asigură supravegherea coordonată a SIS.

2. Aceste autorități, acționând fiecare în limitele competențelor deținute, fac schimb de informații relevante, se asistă reciproc în efectuarea auditurilor și a inspecțiilor, examinează dificultățile legate de interpretarea sau aplicarea prezentului regulament și a altor acte juridice aplicabile ale Uniunii, analizează problemele identificate prin exercitarea supravegherii independente sau prin exercitarea drepturilor persoanelor vizate, elaborează propuneri armonizate în vederea găsirii unor soluții comune la eventualele probleme și promovează sensibilizarea cu privire la drepturile în materie de protecție a datelor, dacă este necesar.

3. În scopurile enunțate la alineatul (2), autoritățile naționale de supraveghere și Autoritatea Europeană pentru Protecția Datelor se reunesc cel puțin de două ori pe an în cadrul Comitetului european pentru protecția datelor, instituit prin Regulamentul (UE) 2016/679. Costurile aferente reuniunilor și organizării acestora sunt suportate de comitetul instituit prin Regulamentul (UE) 2016/679. Regulamentul de procedură se adoptă în cadrul primei reuniuni. Dacă este necesar, se elaborează de comun acord alte metode de lucru.

4. Din doi în doi ani, comitetul instituit prin Regulamentul (UE) 2016/679 trimite Parlamentului European, Consiliului și Comisiei un raport comun privind activitățile de supraveghere coordonată.

CAPITOLUL X

RĂSPUNDEREA

Articolul 53
Răspunderea

1. Fiecare stat membru răspunde pentru eventualele daune cauzate unei persoane ca urmare a utilizării N.SIS. Acest lucru se aplică și daunelor cauzate de statul membru semnalant, în cazul în care acesta din urmă a introdus date care conțin erori de fapt sau a stocat date în mod ilegal.

2. În cazul în care statul membru împotriva căruia se introduce o acțiune nu este statul membru care a emis semnalarea, acesta din urmă rambursează, la cerere, sumele plătite drept compensație, cu excepția cazului în care utilizarea datelor de către statul membru care solicită rambursarea încalcă prezentul regulament.

3. În cazul în care orice nerespectare de către un stat membru a obligațiilor care îi revin în temeiul prezentului regulament provoacă daune SIS, respectivul stat membru

răspunde pentru aceste daune, cu excepția cazului și în măsura în care agenția sau un alt stat membru care participă la SIS nu a luat măsuri rezonabile pentru a preveni producerea daunelor sau pentru a le reduce impactul.

CAPITOLUL XI

DISPOZIȚII FINALE

Articolul 54
Monitorizare și statistici

1. Agenția se asigură că există proceduri pentru a monitoriza funcționarea SIS din perspectiva obiectivelor legate de rezultate, eficacitatea costurilor, securitate și calitatea serviciului.

2. În scopul întreținerii tehnice, al elaborării de rapoarte și al întocmirii de statistici, agenția are acces la informațiile necesare privind operațiunile de prelucrare efectuate în SIS central.

3. Agenția întocmește zilnic, lunar și anual statistici care prezintă numărul de înregistrări pentru fiecare categorie de semnalări, numărul anual de rezultate pozitive pentru fiecare categorie de semnalări, numărul de căutări efectuate în SIS și numărul de accesări ale SIS în scopul introducerii, al actualizării sau al ștergerii unei semnalări, în total și pentru fiecare stat membru, inclusiv statistici privind procedura de consultare menționată la articolul 26. Statisticile întocmite nu conțin date cu caracter personal. Raportul statistic anual se publică.

4. Statele membre, precum și Europol și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă furnizează agenției și Comisiei informațiile necesare pentru elaborarea rapoartelor menționate la alineatele (7) și (8).

5. Agenția furnizează statelor membre, Comisiei, Europol și Agenției Europene pentru Poliția de Frontieră și Garda de Coastă toate rapoartele statistice pe care le elaborează. Pentru a monitoriza punerea în aplicare a actelor juridice ale Uniunii, Comisia este în măsură să solicite agenției să furnizeze rapoarte statistice specifice suplimentare, periodice sau ad-hoc, privind performanța sau utilizarea SIS și a comunicațiilor SIRENE.

6. În sensul prezentului articol alineatele (3)-(5) și al articolului 15 alineatul (5), agenția creează, pune în aplicare și găzduiește în sediile sale tehnice un registru central care conține datele menționate la prezentului articol alineatul (3) și la articolul 15 alineatul (5) care nu fac posibilă identificarea persoanelor și care permite Comisiei și agențiilor menționate la alineatul (5) să obțină rapoarte și statistici speciale. Agenția acordă statelor membre, Comisiei, Europol și Agenției Europene pentru Poliția de Frontieră și Garda de Coastă un acces securizat la registrul central prin intermediul infrastructurii de comunicare cu un control al accesului și profiluri de utilizator specifice, exclusiv în scopul întocmirii de rapoarte și statistici.

   Normele detaliate privind funcționarea registrului central și protecția datelor și normele de securitate aplicabile registrului se stabilesc și se precizează prin

intermediul unor măsuri de punere în aplicare adoptate în conformitate cu procedura de examinare menționată la articolul 55 alineatul (2).

7. La doi ani după intrarea în funcțiune a SIS și ulterior din doi în doi ani, agenția prezintă Parlamentului European și Consiliului un raport privind funcționarea tehnică a SIS central și privind funcționarea infrastructurii de comunicare, inclusiv securitatea acesteia, și schimbul bilateral și multilateral de informații suplimentare dintre statele membre.

8. La trei ani după intrarea în funcțiune a SIS și ulterior din patru în patru ani, Comisia efectuează o evaluare globală a SIS central și a schimbului bilateral și multilateral de informații suplimentare dintre statele membre. Această evaluare globală include o examinare a rezultatelor obținute în raport cu obiectivele și o analiză a menținerii valabilității raționamentului care stă la baza sistemului, a aplicării prezentului regulament în ceea ce privește SIS central, a securității SIS central și a oricăror implicații asupra viitoarelor operațiuni. Comisia transmite evaluarea Parlamentului European și Consiliului.

Articolul 55
Procedura comitetului

1. Comisia este asistată de un comitet. Acesta 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 56

Modificări aduse Regulamentului (UE) nr. 515/2014

Regulamentul (UE) nr. 515/2014[74] se modifică după cum urmează:

La articolul 6, se introduce următorul alineat (6):

„6. În timpul etapei de dezvoltare, statele membre beneficiază, pe lângă alocarea lor de bază, de o finanțare forfetară suplimentară de 36,8 milioane EUR pe care o alocă integral finanțării sistemelor naționale SIS pentru a se asigura actualizarea rapidă și eficace a acestora în conformitate cu punerea în aplicare a SIS central, astfel cum se prevede în Regulamentul (UE) 2018/…[*] și în Regulamentul (UE) 2018/…[**].

[*]*Regulamentul privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală (JO…..)*

[**]Regulamentul (UE) 2018/…privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere (JO…..).”

[74] 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 (JO L 150, 20.5.2014, p. 143).

Articolul 57
Abrogare

Regulamentul (CE) nr. 1987/2006 privind instituirea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație;

Decizia 2010/261/UE a Comisiei din 4 mai 2010 privind planul de securitate pentru SIS II central și infrastructura de comunicații[75];

Articolul 25 din Convenția de punere în aplicare a Acordului Schengen[76].

Articolul 58
Intrarea în vigoare și aplicabilitatea

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

2. Prezentul regulament se aplică de la data stabilită de către Comisie după ce:

   (a) s-au adoptat măsurile necesare de punere în aplicare;

   (b) statele membre au notificat Comisiei faptul că au luat măsurile tehnice și juridice necesare pentru prelucrarea datelor din SIS și efectuarea schimbului de informații suplimentare în temeiul prezentului regulament;

   (c) agenția a notificat Comisiei finalizarea tuturor activităților de testare în ceea ce privește CS-SIS și interacțiunea dintre C.SIS și N-SIS.

3. Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în statele membre, în conformitate cu Tratatul privind funcționarea Uniunii Europene.

Adoptat la Bruxelles,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președintele	*Președintele*

[75] Decizia 2010/261/UE a Comisiei din 4 mai 2010 privind planul de securitate pentru SIS II central și infrastructura de comunicații (JO L 112, 5.5.2010, p. 31).

[76] JO L 239, 22.9.2000, p. 19.

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Denumirea propunerii/inițiativei

1.2. Domeniul (domeniile) de politică în cauză în structura ABM/ABB

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 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere și de abrogare a Regulamentului (CE) nr. 1987/2006.

1.2. Domeniul (domeniile) de politică în cauză în structura ABM/ABB[77]

Domeniul de politică: Migrație și afaceri interne (titlul 18)

1.3. Tipul propunerii/inițiativei

☐ 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

Obiectiv - „Către o nouă politică în domeniul migrației”

Necesitatea de a revizui temeiul juridic al SIS pentru a face față noilor provocări în materie de securitate și migrație a fost subliniată de Comisie în mai multe rânduri. De exemplu, în „Agenda europeană privind migrația”[79], Comisia a declarat că gestionarea mai eficientă a frontierelor presupune, de asemenea, o mai bună valorificare a oportunităților oferite de sistemele și tehnologiile informatice. În „Agenda europeană privind securitatea”[80], Comisia și-a anunțat intenția de a evalua SIS în perioada 2015-2016 și de a analiza posibilitățile de a ajuta statele membre să pună în aplicare interdicțiile de călătorie stabilite la nivel național. În „Planul de acțiune al UE împotriva introducerii ilegale de migranți”[81], Comisia a declarat că analizează impunerea obligației pentru autoritățile statelor membre de a introduce în SIS toate interdicțiile de intrare astfel încât să se asigure respectarea acestora la nivelul întregii UE. În plus, Comisia a declarat, de asemenea, că va analiza posibilitatea și caracterul proporțional al introducerii în SIS a deciziilor de returnare emise de autoritățile statelor membre, pentru a verifica dacă un migrant în situație neregulamentară care a fost reținut face obiectul unei decizii de returnare emise de alt stat membru. În fine, în Comunicarea intitulată „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”[82], Comisia a subliniat că

---

77 ABM (*activity based management*): gestiune pe activități – ABB (*activity based budgeting*): întocmirea bugetului pe activități.

78 Astfel cum sunt menționate la articolul 54 alineatul (2) litera (a) sau (b) din Regulamentul financiar.

79 COM(2015) 240 final.

80 COM(2015) 185 final.

81 COM(2015) 285 final.

82 COM(2016) 205 final.

examinează introducerea unor posibile funcționalități suplimentare în SIS și prezentarea de propuneri de revizuire a temeiului juridic al sistemului.

Ca urmare a evaluării globale a sistemului și în deplină concordanță cu obiectivele multianuale ale Comisiei, prezentate în comunicările menționate mai sus și în Planul strategic pentru perioada 2016-2020 al DG Migrație și Afaceri Interne[83], prezenta propunere vizează reformarea structurii, a funcționării și a utilizării Sistemului de informații Schengen în domeniul verificărilor la frontiere.

1.4.2. Obiectiv(e) specific(e) și activitatea (activitățile) ABM/ABB în cauză

Obiectivul specific nr.

Planul de management pentru 2017 al DG Migrație și Afaceri Interne - obiectivul specific nr. 1.2:

Gestionarea eficace a frontierelor – salvarea de vieți omenești și securizarea frontierelor externe ale UE.

Activitatea (activitățile) ABM/ABB în cauză

Capitolul 18 02 – Securitate internă

[83] Ares(2016)2231546 – 12.5.2016.

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.

Principalele obiective ale politicii sunt următoarele:

1. să contribuie la un nivel ridicat de securitate în spațiul de libertate, securitate și justiție al UE;

2. să sporească eficacitatea și eficiența controalelor la frontiere.

Recomandările formulate în urma evaluării globale a SIS, care a fost efectuată de DG HOME în perioada 2015-2016, vizau aducerea de îmbunătățiri tehnice sistemului și armonizarea procedurilor naționale din domeniul gestionării refuzurilor intrării și ale șederii. De exemplu, actualul Regulament privind SIS II doar permite, dar nu impune statelor membre să introducă în sistem semnalări privind refuzul intrării și al șederii. Unele state membre introduc în mod sistematic în SIS toate interdicțiile de intrare, în timp ce altele nu fac acest lucru. Prin urmare, prezenta propunere va contribui la realizarea unui nivel mai ridicat de armonizare în acest domeniu, prin impunerea obligației de a introduce în SIS toate interdicțiile de intrare, și definește norme comune privind introducerea semnalărilor în sistem și precizarea motivului care stă la baza unei semnalări.

Noua propunere introduce măsuri care abordează nevoile tehnice și operaționale ale utilizatorilor finali. În special, noile câmpuri de date pentru semnalările existente vor permite polițiștilor de frontieră să dispună de toate informațiile necesare pentru a-și îndeplini sarcinile cu eficacitate. În plus, propunerea subliniază în mod specific importanța disponibilității neîntrerupte a SIS, deoarece perioadele de indisponibilitate pot afecta în mod semnificativ capacitatea de a efectua controale la frontierele externe. Prin urmare, prezenta propunere va avea un pronunțat efect pozitiv asupra eficacității controalelor la frontiere.

Odată adoptate și puse în aplicare, aceste propuneri vor permite să se asigure într-o mai mare măsură continuitatea activității – statele membre vor avea obligația de a dispune de o copie națională integrală sau parțială și de un sistem de rezervă. Acest lucru va permite sistemului să rămână pe deplin funcțional și operațional pentru agenții de pe teren.

1.4.4. Indicatori de rezultat și de impact

A se preciza indicatorii care permit monitorizarea punerii în aplicare a propunerii/inițiativei.

În timpul actualizării sistemului

După aprobarea proiectului de propunere și adoptarea specificațiilor tehnice, SIS va fi actualizat pentru a se armoniza mai bine procedurile naționale de utilizare a sistemului, pentru a se extinde domeniul de aplicare al sistemului prin consolidarea nivelurilor de date disponibile utilizatorilor finali în vederea unei informări sporite a agenților care efectuează verificări și pentru a se realiza modificările tehnice menite să îmbunătățească securitatea și să contribuie la reducerea sarcinilor administrative. eu-LISA va coordona gestionarea proiectului de actualizare a sistemului. Agenția va înființa o structură de gestionare a proiectului și va prezenta un calendar detaliat cu etape de referință pentru realizarea modificărilor propuse, ceea ce va permite Comisiei să monitorizeze îndeaproape punerea în aplicare a propunerii.

Obiectiv specific – Funcționalitățile actualizate ale SIS să devină operaționale în 2020.

Indicator – încheierea cu succes a testării cuprinzătoare a sistemului revizuit, înainte de lansarea acestuia.

După ce sistemul începe să funcționeze

După ce sistemul începe să funcționeze, eu-LISA se va asigura că există proceduri pentru a monitoriza funcționarea SIS în raport cu obiectivele legate de rezultate, eficacitatea costurilor, securitate și calitatea serviciului. La doi ani după intrarea în funcțiune a SIS și ulterior din doi în doi ani, eu-LISA are obligația de a prezenta Parlamentului European și Consiliului un raport privind funcționarea tehnică a SIS central și privind funcționarea infrastructurii de comunicare, inclusiv securitatea acesteia, și schimbul bilateral și multilateral de informații suplimentare dintre statele membre. De asemenea, eu-LISA întocmește zilnic, lunar și anual statistici care prezintă numărul de înregistrări pentru fiecare categorie de semnalări, numărul anual de rezultate pozitive pentru fiecare categorie de semnalări, numărul de căutări efectuate în SIS și numărul de accesări ale sistemului în scopul introducerii, al actualizării sau al ștergerii unei semnalări, în total și pentru fiecare stat membru.

La trei ani după intrarea în funcțiune a SIS și ulterior din patru în patru ani, Comisia efectuează o evaluare globală a SIS central și a schimbului bilateral și multilateral de informații suplimentare dintre statele membre. Această evaluare globală include o examinare a rezultatelor obținute în raport cu obiectivele și o analiză a menținerii valabilității raționamentului care stă la baza sistemului, a aplicării prezentului regulament în ceea ce privește SIS central, a securității SIS central și a oricăror implicații asupra viitoarelor operațiuni. Comisia trimite evaluarea Parlamentului European și Consiliului.

1.5. Motivele propunerii/inițiativei

1.5.1. Cerință (cerințe) de îndeplinit pe termen scurt sau lung

1. Contribuirea la menținerea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție al UE.

2. Întărirea luptei împotriva criminalității internaționale, a terorismului și a altor amenințări la adresa securității.

3. Extinderea domeniului de aplicare al SIS prin introducerea unor noi elemente în semnalările privind refuzul intrării și al șederii.

4. Sporirea eficacității controalelor la frontiere.

5. Sporirea eficienței activității polițiștilor de frontieră și a autorităților din domeniul imigrației.

6. Realizarea unui nivel mai ridicat de eficacitate și armonizare a procedurilor naționale și asigurarea respectării interdicțiilor de intrare în spațiul Schengen.

7. Contribuirea la combaterea migrației neregulamentare.

1.5.2. Valoarea adăugată a intervenției UE

SIS este principala bază de date în materie de securitate din Europa. În absența controalelor la frontierele interne, combaterea eficace a criminalității și a terorismului a dobândit o dimensiune europeană. Prin urmare, SIS este indispensabil

pentru a veni în sprijinul controalelor la frontierele externe și al verificărilor privind migranții în situație neregulamentară găsiți pe teritoriul național. Obiectivele prezentei propuneri se referă la îmbunătățirile tehnice menite să sporească eficiența și eficacitatea sistemului și să armonizeze utilizarea acestuia în toate statele membre participante. Caracterul transnațional al obiectivelor, alături de provocările aferente asigurării unui schimb eficace de informații pentru combaterea amenințărilor care se diversifică tot mai mult, fac ca UE să fie cea mai în măsură să propună soluții la aceste probleme. Obiectivele de sporire a eficienței și a utilizării armonizate a SIS, și anume creșterea volumului, a calității și a vitezei schimbului de informații prin intermediul unui sistem centralizat de informații la scară largă gestionat de o agenție de reglementare (eu-LISA), nu pot fi realizate de statele membre în mod individual și necesită o intervenție la nivelul UE. Dacă aspectele propuse nu sunt puse în aplicare, SIS va continua să funcționeze în conformitate cu normele aplicabile în prezent, pierzându-se astfel oportunități de maximizare a eficienței și a valorii adăugate a UE identificate prin intermediul evaluării SIS și a utilizării acestuia de către statele membre.

Doar în 2015, autoritățile naționale au efectuat aproape 2,9 miliarde de căutări în SIS și au făcut schimb de peste 1,8 milioane de informații suplimentare, ceea ce demonstrează în mod clar contribuția esențială a sistemului la controalele la frontierele externe. Acest nivel ridicat al schimbului de informații dintre statele membre nu ar fi fost atins prin intermediul unor soluții descentralizate și ar fi fost imposibil să se obțină aceste rezultate la nivel național. În plus, SIS s-a dovedit a fi cel mai eficace instrument de schimb de informații în scopul combaterii terorismului și oferă valoarea adăugată a UE prin faptul că permite serviciilor de securitate naționale să coopereze într-un mod rapid, confidențial și eficient. Noile propuneri vor facilita și mai mult schimbul de informații și cooperarea dintre autoritățile de control la frontiere din statele membre ale UE. În plus, Europol și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă vor beneficia, în limitele competențelor de care dispun, de acces deplin la sistem, ceea ce demonstrează în mod clar valoarea adăugată a intervenției UE.

1.5.3. Învățăminte desprinse din experiențe anterioare similare

Principalele învățăminte desprinse în urma dezvoltării Sistemului de informații Schengen de a doua generație au fost următoarele:

1. Faza de dezvoltare ar trebui să înceapă numai după definirea integrală a cerințelor tehnice și operaționale. Dezvoltarea poate avea loc numai după adoptarea definitivă a instrumentelor juridice care stau la baza sistemului și care îi stabilesc scopul, domeniul de aplicare, funcțiile și detaliile tehnice.

2. În cadrul procedurii de comitologie, Comisia a efectuat (și continuă să efectueze) consultări frecvente cu părțile interesate relevante, inclusiv delegații la Comitetul SISVIS. Din acest comitet fac parte reprezentanți ai statelor membre atât în ceea ce privește chestiunile operaționale referitoare la SIRENE (cooperarea transfrontalieră în legătură cu SIS), cât și în ceea ce privește chestiunile tehnice în materie de dezvoltare și întreținere a SIS și a aplicației SIRENE conexe. Modificările propuse de prezentul regulament au fost discutate în mod transparent și cuprinzător în cadrul unor reuniuni și ateliere specifice. De asemenea, pe plan intern, Comisia a înființat un grup de coordonare între servicii, din care au făcut parte Secretariatul General, Direcția Generală Migrație și Afaceri Interne, Direcția Generală Justiție și Consumatori, Direcția Generală Resurse Umane și Securitate și Direcția Generală

Informatică. Acest grup de coordonare a monitorizat procesul de evaluare și a oferit orientări, după caz.

3. Comisia a solicitat, de asemenea, expertiză externă, comandând trei studii, ale căror constatări au fost utilizate la elaborarea prezentei propuneri:

- Evaluarea tehnică a SIS (*SIS Technical Assessment*) (Kurt Salmon) – evaluarea a identificat principalele probleme ale SIS și nevoile viitoare care ar trebui avute în vedere; aceasta a identificat preocupările în ceea ce privește maximizarea asigurării continuității activității și garantarea faptului că arhitectura globală se poate adapta la creșterea cerințelor de capacitate;

- Evaluarea impactului în materie de TIC al posibilelor îmbunătățiri ale arhitecturii SIS II (*ICT Impact Assessment of Possible Improvements to the SIS II Architecture*) (Kurt Salmon) – studiul a evaluat costul actual al funcționării SIS la nivel național și a analizat trei scenarii tehnice posibile de îmbunătățire a sistemului. Toate scenariile includ o serie de propuneri tehnice axate pe îmbunătățirea sistemului central și a arhitecturii globale;

- Studiu privind fezabilitatea și implicațiile creării în cadrul Sistemului de informații Schengen a unui sistem la nivelul UE pentru schimbul de date privind deciziile de returnare și pentru monitorizarea respectării acestor decizii (*Study on the feasibility and implications of setting up within the framework of the Schengen Information System an EU-wide system for exchanging data on and monitoring compliance with return decisions*) (PwC) - acest studiu evaluează fezabilitatea și implicațiile tehnice și operaționale ale modificărilor propuse care vizează ca SIS să fie utilizat în mai mare măsură pentru returnarea migranților în situație neregulamentară și pentru a împiedica reintrarea lor.

1.5.4. Compatibilitatea și posibila sinergie cu alte instrumente corespunzătoare

Prezenta propunere ar trebui să fie considerată ca punerea în aplicare a acțiunilor prevăzute în Comunicarea din 6 aprilie 2016, intitulată „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”[84], care subliniază necesitatea ca UE să își consolideze și să își îmbunătățească sistemele informatice, arhitectura de date și schimbul de informații în domeniul asigurării respectării legii, al combaterii terorismului și al gestionării frontierelor.

În plus, propunerea este coerentă cu o serie de politici ale Uniunii în acest domeniu:

a) securitatea internă, în ceea ce privește rolul SIS de prevenire a intrării resortisanților țărilor terțe care reprezintă o amenințare la adresa securității;

b) protecția datelor, în măsura în care prezenta propunere asigură protecția drepturilor fundamentale la respectarea vieții private a persoanelor ale căror date cu caracter personal sunt prelucrate în SIS.

Propunerea este, de asemenea, compatibilă cu legislația existentă a Uniunii Europene, și anume instrumentele referitoare la:

a) o politică de returnare eficace a UE, care contribuie la sistemul UE de depistare și prevenire a reintrării resortisanților țărilor terțe după returnarea lor și care întărește acest sistem. O astfel de măsură ar înlesni reducerea stimulentelor pentru migrația neregulamentară către UE, unul dintre principalele obiective ale Agendei europene

[84] COM(2016) 205 final.

privind migrația[85]; b) **Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă[86]**: în ceea ce privește posibilitatea ca personalul agenției care efectuează analize ale riscurilor, precum și echipele europene de poliție de frontieră și gardă de coastă, echipele de personal implicat în sarcini legate de returnare și membrii echipelor de sprijin pentru gestionarea migrației să aibă dreptul, în limitele mandatului lor, de a accesa și de a efectua căutări în datele introduse în SIS;

c) controalele la frontierele externe, în măsura în care prezentul regulament acordă sprijin statelor membre pentru controlarea părții lor din frontierele externe ale UE și pentru întărirea încrederii în eficacitatea sistemului UE de gestionare a frontierelor;

d) **Europol**, în măsura în care propunerea acordă Europol drepturi suplimentare de acces la datele introduse în SIS și de efectuare de căutări în aceste date, în limitele mandatului său.

Propunerea este, de asemenea, compatibilă cu viitoarea legislație a Uniunii Europene, și anume instrumentele referitoare la:

a) **sistemul de intrare/ieșire[87]**, care propune o combinație de amprente digitale și imagini faciale ca elemente biometrice de identificare pentru funcționarea sistemului de intrare/ieșire (EES); prezenta propunere urmărește să reflecte această abordare;

b) ETIAS, care a propus o evaluare aprofundată în materie de securitate, inclusiv o verificare în SIS, a resortisanților țărilor terțe care intenționează să călătorească în UE și care sunt exonerați de obligația de a deține viză.

85 COM(2015) 240 final.

86 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).

87 Propunerea de regulament al Parlamentului European și al Consiliului de instituire a sistemului de intrare/ieșire (EES) pentru înregistrarea datelor de intrare și de ieșire și a datelor referitoare la refuzul intrării în ceea ce îi privește pe resortisanții țărilor terțe care trec frontierele externe ale statelor membre ale Uniunii Europene, de stabilire a condițiilor de acces la EES în scopul asigurării respectării legii și de modificare a Regulamentului (CE) nr. 767/2008 și a Regulamentului (UE) nr. 1077/2011 [COM(2016) 194 final].

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**

– Punere în aplicare cu o perioadă de creștere în intensitate din 2018 până în 2020,

– urmată de o perioadă de funcționare în regim de croazieră.

1.7. Modul (modurile) de gestiune preconizat(e)[88]

☑ **Gestiune directă** asigurată de către Comisie

– ☑ 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

Comisia va fi responsabilă cu gestionarea globală a politicii, iar eu-LISA va fi responsabilă cu dezvoltarea, funcționarea și întreținerea sistemului.

SIS constituie un sistem de informații unic. În consecință, cheltuielile prevăzute în două propuneri [prezenta propunere și Propunerea de regulament privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală] nu ar trebui considerate ca fiind două cuantumuri distincte, ci ca unul singur. Implicațiile bugetare

[88] Explicațiile privind modurile de gestiune, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

ale modificărilor necesare pentru punerea în aplicare a ambelor propuneri sunt incluse într-o singură fișă financiară legislativă.

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

A se preciza frecvența și condițiile aferente acestor dispoziții.

Comisia, statele membre și agenția vor reexamina și monitoriza în mod regulat utilizarea SIS, pentru a se asigura că acesta continuă să funcționeze în mod eficace și eficient. Comisia va fi asistată de Comitet pentru a pune în aplicare măsurile tehnice și operaționale prezentate în prezenta propunere.

În plus, la articolul 54 alineatele (7) și (8), prezenta propunere de regulament include dispoziții privind un proces de revizuire și evaluare formal și regulat.

Din doi în doi ani, eu-LISA trebuie să prezinte un raport Parlamentului European și Consiliului privind funcționarea tehnică - inclusiv securitatea - SIS, infrastructura de comunicare ce stă la baza acestuia și schimbul bilateral și multilateral de informații suplimentare între statele membre.

În plus, din patru în patru ani, Comisia trebuie să efectueze o evaluare globală a SIS și a schimbului de informații dintre statele membre, pe care o transmite Parlamentului și Consiliului. Aceasta va:

a) examina rezultatele obținute în raport cu obiectivele;

b) evalua dacă raționamentul care stă la baza sistemului rămâne valabil;

c) examina modul în care regulamentul este aplicat în ceea ce privește sistemul central;

d) evalua securitatea sistemului central;

e) analiza implicațiile pentru funcționarea în viitor a sistemului.

2.2. De asemenea, eu-LISA are acum și obligația de a furniza statistici zilnice, lunare și anuale privind utilizarea SIS și asigurarea monitorizării continue a sistemului și a funcționării sale în raport cu obiectivele. Sistemul de gestiune și de control

2.2.1. Riscul (riscurile) identificat(e).

Au fost identificate următoarele riscuri:

1. Eventualele dificultăți întâmpinate de eu-LISA în gestionarea dezvoltărilor prezentate în prezenta propunere în paralel cu alte dezvoltări în curs (de exemplu, punerea în aplicare a AFIS în cadrul SIS) și dezvoltări viitoare (de exemplu, sistemul de intrare-ieșire, ETIAS și actualizarea Eurodac). Acest risc ar putea fi atenuat prin asigurarea faptului că eu-LISA dispune de personal și resurse suficiente pentru îndeplinirea acestor sarcini și gestionarea permanentă a relației cu contractantul responsabil cu menținerea în stare de funcționare a sistemului.

2. Dificultăți întâmpinate de statele membre:

2.1. Aceste dificultăți sunt în primul rând de natură financiară. De exemplu, propunerile legislative includ dezvoltarea obligatorie a unei copii naționale parțiale în fiecare N.SIS II. Statele membre care nu au dezvoltat deja o astfel de copie, vor trebui să facă investițiile necesare. În mod similar, punerea în aplicare la nivel național a documentului de control al interfeței ar fi trebuit să se fi încheiat. Statele membre care nu au făcut încă acest lucru vor trebui să aloce fonduri în bugetele ministerelor vizate. Acest risc ar putea fi atenuat prin furnizarea de finanțare din

partea UE pentru statele membre, de exemplu din componenta destinată frontierelor din cadrul Fondului pentru securitate internă (FSI).

2.2. Sistemele naționale trebuie să fie aliniate la cerințele sistemului central și discuțiile cu statele membre privind acest aspect pot duce la înregistrarea de întârzieri în procesul de dezvoltare. Acest risc ar putea fi atenuat printr-o cooperare timpurie cu statele membre privind alinierea în vederea asigurării faptului că se pot lua măsuri în timp util.

2.2.2. Informații privind sistemul de control intern instituit

eu-LISA este responsabilă de componentele centrale ale SIS. Pentru a permite o mai bună monitorizare a utilizării SIS în scopul de a analiza tendințele privind presiunea migrației, gestionarea frontierelor și infracțiunile, agenția ar trebui să fie în măsură să dezvolte un sistem conform cu stadiul actual al tehnologiei în vederea elaborării de rapoarte statistice destinate statelor membre și Comisiei.

Conturile eu-LISA vor fi supuse aprobării Curții de Conturi și vor face obiectul procedurii de descărcare de gestiune. Serviciul de Audit Intern al Comisiei va efectua audituri în cooperare cu auditorul intern al agenției.

2.2.3. Estimarea costurilor și a beneficiilor controalelor și evaluarea nivelului prevăzut de risc de eroare

Nu se aplică.

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. Agenția aderă la Acordul interinstituțional privind investigațiile interne efectuate de Oficiul European de Luptă Antifraudă (OLAF) și prevede, fără întârziere, dispozițiile corespunzătoare aplicabile tuturor angajaților agenției.

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 la beneficiarii finanțărilor acordate de agenție și la agenții 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 termenii 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

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			
	[Rubrica 3 – Securitate și cetățenie	Dif./Nedif.[89]	Țări AELS[90]	Țări candidate[91]	Țări terțe	În sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar
	18.0208 – Sistemul de informații Schengen	Dif.	NU	NU	DA	NU
	18.020101 – Sprijin pentru gestionarea frontierelor și o politică comună în domeniul vizelor în scopul de a facilita călătoriile legitime	Dif.	NU	NU	DA	NU
	18.0207 – 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

[89] Dif. = credite diferențiate / Nedif. = credite nediferențiate.

[90] AELS: Asociația Europeană a Liberului Schimb.

[91] Țările candidate și, după caz, țările potențial candidate din Balcanii de Vest.

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

Rubrica din cadrul financiar multianual:	3	Securitate și cetățenie

DG HOME			Anul **2018**	Anul **2019**	Anul **2020**	**TOTAL**
• Credite operaționale						
18.0208 Sistemul de informații Schengen	Angajamente	(1)	6,234	1,854	1,854	**9,942**
	Plăți	(2)	6,234	1,854	1,854	**9,942**
18.020101 (Frontiere și vize)	Angajamente	(1)		18,405	18,405	**36,810**
	Plăți	(2)		18,405	18,405	**36,810**
TOTAL credite pentru DG HOME	Angajamente	=1+1a +3	6,234	20,259	20,259	**46,752**
	Plăți	=2+2a +3	6,234	20,259	20,259	**46,752**

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual:	3	Securitate și cetățenie

eu-LISA			Anul **2018**	Anul **2019**	Anul **2020**	**TOTAL**
• Credite operaționale						
Titlul 1: Cheltuieli cu personalul	Angajamente	(1)	0,210	0,210	0,210	**0,630**
	Plăți	(2)	0,210	0,210	0,210	**0,630**
Titlul 2: Cheltuieli de infrastructură și de funcționare	Angajamente	(1a)	0	0	0	**0**
	Plăți	(2a)	0	0	0	**0**
Titlul 3: Cheltuieli operaționale	Angajamente	(1a)	12,893	2,051	1,982	**16,926**
	Plăți	(2a)	2,500	7,893	4,651	**15,044**
TOTAL credite pentru eu-LISA	Angajamente	=1+1a +3	13,103	2,261	2,192	**17,556**
	Plăți	=2+2a +3	2,710	8,103	4,861	**15,674**

3.2.2. Impactul estimat asupra creditelor operaționale

• TOTAL credite operaționale	Angajamente	(4)								
	Plăți	(5)								
• TOTAL credite cu caracter administrativ finanțate din bugetul anumitor programe		(6)								

TOTAL credite în cadrul RUBRICII <….> din cadrul financiar multianual	Angajamente	=4+ 6								
	Plăți	=5+ 6								

În cazul în care propunerea/inițiativa afectează mai multe rubrici:

• TOTAL credite operaționale	Angajamente	(4)							
	Plăți	(5)							
• TOTAL credite cu caracter administrativ finanțate din bugetul anumitor programe		(6)							
TOTAL credite în cadrul RUBRICILOR 1-4 din cadrul financiar multianual (Suma de referință)	Angajamente	=4+ 6	19,337	22,520	22,451				**64,308**
	Plăți	=5+ 6	8,944	28,362	25,120				**62,426**

3.2.3. Impactul estimat asupra creditelor cu caracter administrativ

Rubrica din cadrul financiar multianual:	**5**	„Cheltuieli administrative”

milioane EUR (cu trei zecimale)

		Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)			**TOTAL**
DG: <…….>									
• Resursele umane									
• Alte cheltuieli administrative									
TOTAL DG <…….>	Credite								

TOTAL credite pentru RUBRICA 5 din cadrul financiar multianual	(Total angajamente = Total plăți)								

milioane EUR (cu trei zecimale)

		Anul **N**[92]	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)			**TOTAL**
TOTAL credite în cadrul RUBRICILOR 1-5 din cadrul financiar multianual	Angajamente								
	Plăți								

[92] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei.

3.2.3.1 Impactul estimat asupra creditelor operaționale ale eu-LISA

– ☐ Propunerea/inițiativa nu implică utilizarea de credite operaționale

– ☑ Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos:

A se indica obiectivele și realizările ⇩			Anul **2018**		Anul **2019**		Anul **2020**		A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)						**TOTAL**			
	REALIZĂRI																	
	Tip[93]	Costuri medii	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 1[94] Dezvoltarea sistemului central																		
- Contractant			1	5,013														5,013
- Software			1	4,050														4,050
- Hardware			1	3,692														3,692
Subtotal pentru obiectivul specific nr. 1				12,755														12,755
OBIECTIVUL SPECIFIC NR. 2 Întreținerea sistemului central																		
- Contractant			1	0	1	0,365	1	0,365										0,730
Software			1	0	1	0,810	1	0,810										1,620
Hardware			1	0	1	0,738	1	0,738										1,476
Subtotal pentru obiectivul specific						1,913		1,913										3,826

[93] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de străzi construiți etc.).

[94] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

nr. 2																
OBIECTIVUL SPECIFIC NR. 3 Reuniuni/formări																
Activități de formare	1	0,138	1	0,138	1	0,069										0,345
Subtotal pentru obiectivul specific nr. 3		0,138		0,138		0,069										0,345
COSTURI TOTALE		12,893		2,051		1,982										16,926

Credite de angajament în milioane EUR (cu trei zecimale)

3.2.3.2 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:

A se indica obiectivele și realizările ⇩			Anul **2018**		Anul **2019**		Anul **2020**		A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)						**TOTAL**			
	REALIZĂRI																	
	Tip[95]	Costuri medii	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 1[96] Dezvoltarea sistemului național			1		1	1,221	1	1,221										2,442
OBIECTIVUL SPECIFIC NR. 2 Infrastructură			1		1	17,184	1	17,184										34,368
COSTURI TOTALE						18,405		18,405										36,810

95 Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de străzi construiți etc.).

96 Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

3.2.3.3 Impactul estimat asupra resurselor umane ale eu-LISA - 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 **2018**	Anul **2019**	Anul **2020**	**TOTAL**
Funcționari (grade AD)				
Funcționari (grade AST)				
Agenți contractuali	0,210	0,210	0,210	0,630
Agenți temporari				
Experți naționali detașați				
TOTAL	**0,210**	**0,210**	**0,210**	**0,630**

Recrutarea este planificată pentru luna ianuarie 2018. Întregul personal trebuie să fie disponibil încă de la începutul anului 2018 pentru ca faza de dezvoltare să poată începe în timp util, astfel încât să se asigure intrarea în funcțiune a SIS II reformat în 2020. Cei 3 noi agenți contractuali sunt necesari pentru a acoperi nevoile atât în ceea ce privește punerea în aplicare a proiectului, cât și sprijinul operațional și întreținerea după intrarea în funcțiune. Aceste resurse vor fi utilizate pentru:

- a sprijini punerea în aplicare a proiectului în calitate de membru al echipei de proiect, inclusiv activități cum ar fi: definirea cerințelor și a specificațiilor tehnice, cooperarea cu statele membre și acordarea de asistență acestora în perioada de punere în aplicare; actualizări ale documentului de control al interfeței (DCI), monitorizarea livrărilor prevăzute în contract, furnizarea de documentație și actualizări etc.;
- sprijinirea activităților de tranziție pentru punerea în funcțiune a sistemului în cooperare cu contractantul [monitorizarea noilor versiuni lansate, actualizările procesului operațional, cursuri de formare (inclusiv activități de formare organizate în statele membre) etc.];
- sprijinirea activităților pe termen mai lung, definirea specificațiilor, pregătiri contractuale în cazul în care este necesară o reconfigurare a sistemului (de exemplu datorită recunoașterii imaginilor) sau în cazul în care vor trebui aduse amendamente noului contract de menținere în stare de funcționare a SIS II pentru a acoperi modificări suplimentare (dintr-o perspectivă tehnică și bugetară);
- consolidarea asistenței de al doilea nivel după intrarea în funcțiune, în timpul întreținerii continue și al desfășurării operațiunilor.

Trebuie remarcat faptul că cei trei noi membri ai personalului (AC ENI) se vor adăuga resurselor echipelor interne care vor fi, de asemenea, alocate proiectului/monitorizării contractuale și financiare/activităților operaționale. Utilizarea agenților contractuali va asigura durata corespunzătoare și continuitatea contractelor pentru a garanta continuitatea activității și utilizarea acelorași persoane specializate pentru activitățile de sprijin operațional după încheierea proiectului. În plus, pentru activitățile de sprijin operațional este necesar accesul la mediul de producție, care nu poate fi acordat contractanților sau personalului extern.

3.2.3.4 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 **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)		
• **Posturi din schema de personal (funcționari și agenți temporari)**								
XX 01 01 01 (la sediu și în birourile de reprezentare ale Comisiei)								
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)**[97]								
XX 01 02 01 (AC, END, INT din „pachetul global”)								
XX 01 02 02 (AC, AL, END, INT și JED în delegații)								
XX 01 04 **yy** [98]	- la sediu							
	- 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								

XX 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:

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

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

Funcționari și personal temporar	
Personal extern	

3.2.4. 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.

Se preconizează o reprogramare a restului pachetului financiar destinat frontierelor inteligente din cadrul Fondului pentru securitate internă în vederea punerii în aplicare a funcționalităților și a modificărilor prevăzute în cele două propuneri. Regulamentul de instituire în cadrul FSI a sprijinului pentru frontiere este instrumentul financiar în care a fost inclus bugetul alocat punerii în aplicare a pachetului privind frontierele inteligente. Articolul 5 prevede că un buget de 791 de milioane EUR va fi executat printr-un program pentru dezvoltarea de sisteme informatice în vederea gestionării fluxurilor migratorii la frontierele externe, în condițiile prevăzute la articolul 15. Din cele 791 de milioane EUR menționate mai sus, 480 de milioane EUR sunt rezervate pentru dezvoltarea sistemului de intrare-ieșire și 210 milioane EUR pentru dezvoltarea sistemului european de informații și de autorizare privind călătoriile (ETIAS). Suma rămasă, și anume 100,828 milioane EUR, va fi utilizată parțial pentru a acoperi costurile aferente modificărilor prevăzute în cele două propuneri privind SIS.

– ☐ Propunerea/inițiativa necesită recurgerea la instrumentul de flexibilitate sau la revizuirea cadrului financiar multianual.

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

3.2.5. Contribuția terților

– ☑ Propunerea/inițiativa nu prevede cofinanțare din partea terților.

– Propunerea/inițiativa prevede cofinanțare, estimată în cele ce urmează:

Credite de angajament în milioane EUR (cu trei zecimale)

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

3.3. Impactul estimat asupra veniturilor

– ☐ Propunerea/inițiativa nu are impact financiar asupra veniturilor.

– ☑ Propunerea/inițiativa are următorul impact financiar:

– – ☐ asupra resurselor proprii

– – ☑ asupra diverselor venituri

milioane EUR (cu trei zecimale)

Linia bugetară pentru venituri:	Credite disponibile pentru exercițiul financiar în curs	Impactul propunerii/inițiativei[99]						
		2018	2019	2020	2021	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)		
Articolul 6313 – Alte contribuții în cadrul acquis-ului Schengen (CH, NO, LI și IS).		p.m.	p.m.	p.m.	p.m.			

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

18.02.08 (Sistemul de Informații Schengen), 18.02.07 (eu-LISA)

A se preciza metoda de calcul a impactului asupra veniturilor.

Bugetul include o contribuție din partea țărilor asociate la punerea în aplicare, asigurarea respectării și dezvoltarea acquis-ului Schengen.

[99] 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 costuri de colectare.