



Bruxelles, 21.12.2016  
COM(2016) 883 final

2016/0409 (COD)

Propunere de

**REGULAMENT 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, de modificare a Regulamentului (UE) nr. 515/2014 și de abrogare a Regulamentului (CE) nr. 1986/2006, a Deciziei 2007/533/JAI a Consiliului și a Deciziei 2010/261/UE a Comisiei**

## **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<sup>1</sup>, 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 completează propunerea privind gestionarea frontierelor și dispozițiile conținute de aceasta,

---

<sup>1</sup> 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...).

stabilind o nouă categorie de semnalări și contribuind la punerea în aplicare și la monitorizarea Directivei 2008/115/CE<sup>2</sup>.

Data 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”<sup>3</sup>. 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<sup>4</sup>. 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<sup>5</sup> 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.

Prezenta propunere face parte dintr-un prim set de propuneri<sup>6</sup> care vizează îmbunătățirea funcționării SIS, precum și a exploatării și a utilizării acestuia în domeniul cooperării polițienești și al cooperării judiciare în materie penală. Aceasta pune în aplicare:

- (1) anunțul Comisiei privind îmbunătățirea valorii adăugate a SIS în scopul asigurării respectării legii<sup>7</sup> pentru a răspunde noilor amenințări;

---

<sup>2</sup> 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).

<sup>3</sup> COM(2016) 205 final, 6.4.2016.

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

<sup>5</sup> 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).

<sup>6</sup> Regulamentul (UE) 2018/xxx [verificări la frontiere] și Regulamentul (UE) 2018/xxx [returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală].

- (2) 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;
- (3) recomandările privind modificările tehnice și procedurale care rezultă dintr-o evaluare cuprinzătoare a SIS<sup>8</sup>;
- (4) solicitările privind îmbunătățiri tehnice primite din partea utilizatorilor finali ai SIS și
- (5) constatările provizorii ale Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate<sup>9</sup> 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 verificărilor la frontiere, o serie de dispoziții sunt comune ambelor texte. Printre acestea se numără măsuri referitoare la utilizarea SIS de la un capăt la altul (*end-to-end*), 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 privind măsuri de monitorizare, de evaluare și de raportare. Ambele propuneri extind, de asemenea, utilizarea informațiilor biometrice<sup>10</sup>.

Cadrul juridic actual al SIS de a doua generație - în ceea ce privește utilizarea sa în scopul cooperării polițienești și al cooperării judiciare în materie penală - se bazează pe un instrument aferent fostului al treilea pilon, și anume Decizia 2007/533/JAI a Consiliului<sup>11</sup>, precum și pe un instrument aferent fostului prim pilon, și anume Regulamentul (CE) nr. 1986/2006<sup>12</sup>. Prezenta propunere consolidează conținutul instrumentelor existente, adăugând totodată dispoziții noi pentru:

- a armoniza mai bine procedurile naționale de utilizare a SIS, în special în ceea ce privește infracțiunile legate de terorism, precum și copiii expuși riscului de a fi răpiți de unul dintre părinți;
- a extinde domeniul de aplicare al SIS prin adăugarea unor noi elemente biometrice de identificare la semnalările existente;
- a introduce modificări tehnice pentru a îmbunătăți securitatea și a contribui la reducerea sarcinii administrative prin impunerea obligației de a avea copii naționale și standarde tehnice comune de punere în aplicare;

<sup>7</sup> A se vedea Comunicarea „Punerea în aplicare a Agendei europene privind securitatea pentru a combate terorismul și a deschide calea către o uniune a securității efectivă și autentică”, p. 4 și următoarele, COM(2016) 230 final, 20.4.2016.

<sup>8</sup> 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...).

<sup>9</sup> Grupul de experți la nivel înalt - Raportul președintelui din 21 decembrie 2016.

<sup>10</sup> Pentru o explicație detaliată a modificărilor incluse în prezenta propunere, a se vedea secțiunea 5 intitulată „Elemente diverse”.

<sup>11</sup> 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).

<sup>12</sup> Regulamentul (CE) nr. 1986/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind accesul la Sistemul de Informații Schengen din a doua generație (SIS II) al serviciilor competente, în statele membre, pentru eliberarea certificatelor de înmatriculare a vehiculelor (JO L 381, 28.12.2006, p. 1).

- a aborda utilizarea completă a SIS de la un capăt la altul, care include nu numai sistemul central și sistemele naționale, ci și asigură faptul că utilizatorii finali primesc toate datele necesare pentru a-și îndeplini sarcinile și respectă toate normele de securitate atunci când prelucrează date din SIS.

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

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

- (1) **securitatea internă**, astfel cum s-a subliniat în Agenda europeană privind securitatea<sup>13</sup> și în cadrul activității Comisiei în vederea realizării unei uniuni a securității efective și autentice<sup>14</sup>, al cărei scop este de a preveni, a depista, a investiga și a urmări penal infracțiunile de terorism și alte infracțiuni grave, permițând autorităților de asigurare a respectării legii să prelucreze datele cu caracter personal ale persoanelor suspectate de a fi implicate în acte de terorism sau în infracțiuni grave;
- (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.

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

- (3) **Poliția de frontieră și garda de coastă la nivel european**, în ceea ce privește accesul său la SIS în scopurile sistemului european de informații și de autorizare privind călătoriile (ETIAS)<sup>15</sup> propus, precum și în scopul de a furniza o interfață tehnică pentru accesul la 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 astfel încât, în limitele mandatului lor, acestea să aibă dreptul de a accesa și de a efectua căutări în datele introduse în SIS;
- (4) **Europol**, în măsura în care prezenta propunere acordă Europol drepturi suplimentare de acces la datele introduse în SIS și de efectuare de căutări în aceste date, în limitele mandatului său;
- (5) **Prüm**, în măsura în care dezvoltările prevăzute în prezenta propunere menite să permită identificarea persoanelor pe baza amprentelor digitale (precum și pe baza imaginilor faciale și a profilurilor ADN) completează dispozițiile Prüm existente<sup>16</sup> privind accesul online transfrontalier reciproc la bazele de date ADN și sistemele automate de identificare a amprentelor digitale naționale desemnate.

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:

---

<sup>13</sup> COM(2015) 185 final.

<sup>14</sup> COM(2016) 230 final.

<sup>15</sup> COM(2016) 731 final.

<sup>16</sup> Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008, p. 1) și Decizia 2008/616/JAI a Consiliului din 23 iunie 2008 privind punerea în aplicare a Deciziei 2008/615/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008, p. 12).

- (6) **gestionarea frontierelor externe** – propunerea completează noul principiu preconizat în Codul frontierelor Schengen, astfel cum a fost instituit ca răspuns la fenomenul luptătorilor teroriști străini, privind efectuarea de verificări sistematice, în bazele de date relevante, ale tuturor călătorilor, inclusiv ale cetățenilor UE, la intrarea și la ieșirea din spațiul Schengen;
- (7) **sistemul de intrare/ieșire** – propunerea urmărește să reflecte utilizarea unei combinații de amprente digitale și imagini faciale ca elemente biometrice de identificare, care a fost propusă pentru funcționarea sistemului de intrare/ieșire (EES);
- (8) **ETIAS** – propunerea ține seama de sistemul ETIAS propus care prevede o evaluare aprofundată în materie de securitate, inclusiv o verificare în SIS, a resortisanților țărilor terțe care intenționează să călătorească în UE.

## 2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

### • Temeiul juridic

Prezenta propunere utilizează articolul 82 alineatul (1) litera (d), articolul 85 alineatul (1), articolul 87 alineatul (2) litera (a) și articolul 88 alineatul (2) litera (a) din Tratatul privind funcționarea Uniunii Europene ca temei juridic pentru dispozițiile referitoare la cooperarea polițienească și cooperarea judiciară în materie penală.

### • Geometrie variabilă

Prezenta propunere constituie o dezvoltare a acquis-ului Schengen privind cooperarea polițienească și cooperarea judiciară în materie penală. 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: Regatul Unit are obligații în temeiul prezentului regulament în conformitate cu articolul 5 din Protocolul privind acquis-ul Schengen integrat în cadrul Uniunii Europene, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, și în conformitate cu articolul 8 alineatul (2) din 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<sup>17</sup>.

Irlanda: Irlanda are obligații în temeiul prezentului regulament în conformitate cu articolul 5 din Protocolul privind acquis-ul Schengen integrat în cadrul Uniunii Europene, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, și în conformitate cu articolul 6 alineatul (2) din Decizia 2002/192/CE a Consiliului din 28 februarie 2002 privind solicitarea Irlandei de a participa la unele dintre dispozițiile acquis-ului Schengen<sup>18</sup>.

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

---

<sup>17</sup> JO L 131, 1.6.2000, p. 43.

<sup>18</sup> JO L 64, 7.3.2002, p. 20.

din 2005. Prezentul regulament trebuie coroborat cu Decizia 2010/365/UE a Consiliului din 29 iunie 2010<sup>19</sup> 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.

Nivelul considerabil al schimbului de informații dintre statele membre prin intermediul SIS 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.

- **Proportionalitatea**

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 reprezintă o revizuire a SIS în ceea ce privește cooperarea polițienească și cooperarea judiciară în materie penală.

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

---

<sup>19</sup> 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).

este absolut necesar pentru a permite sistemului să funcționeze și să își îndeplinească obiectivele. Pe baza cerințelor operaționale, prezenta propunere reduce perioada de păstrare a semnalărilor privind obiecte și le aliniază la semnalările privind persoane (deoarece, de multe ori, semnalările privind obiecte au legătură cu date cu caracter personal, cum ar fi documente de identificare personale sau plăcuțe de înmatriculare). Experiența polițienească arată că un bun furat poate fi recuperat într-o perioadă relativ scurtă de timp, ceea ce face ca termenul de 10 ani de expirare a valabilității unei semnalări privind obiecte să fie inutil de lung.

Semnalările din 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 forma unui regulament și va înlocui Decizia 2007/533/JAI a Consiliului, menținând în același timp o mare parte din conținutul deciziei menționate. 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 colegiutor. 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<sup>20</sup> (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.

<sup>20</sup>

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).

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, 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.

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 de a aborda SIS dintr-o perspectivă care să meargă de la un capăt la altul, prin reglementarea folosirii sale de către utilizatorii finali și stabilirea de standarde de securitate a datelor pe care să le respecte și aplicațiile destinate utilizatorilor finali, de a întări sistemul în scopuri de combatere a terorismului, prin stabilirea unei noi acțiuni care trebuie întreprinse, de a clarifica situația copiilor care sunt în pericol de a fi răpiți de către părinții lor, precum și de a extinde elementele biometrice de identificare disponibile în sistem.

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 conexe au fost adoptate la 21 decembrie 2016<sup>21</sup>) au constituit baza măsurilor incluse în prezenta propunere.

- **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 67 din Decizia 2007/533/JAI a Consiliului, 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

---

<sup>21</sup> 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

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.

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 trei studii, ale căror constatări au fost utilizate la elaborarea prezentei propuneri:

- Evaluarea tehnică a SIS (*SIS Technical Assessment*) (Kurt Salmon)<sup>22</sup>

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)<sup>23</sup>

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)<sup>24</sup>

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).

---

<sup>22</sup> Comisia Europeană, RAPORT FINAL - Evaluarea tehnică a SIS II (*FINAL REPORT - SIS II technical assessment*).

<sup>23</sup> 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.

<sup>24</sup> 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).

- **Evaluarea impactului**

Comisia nu a efectuat o evaluare a impactului.

Cele trei evaluări independente menționate mai sus (în secțiunea „Obținerea și utilizarea expertizei”) au stat la baza analizei din punct de vedere tehnic a impacturilor modificărilor propuse a fi aduse sistemului. În plus, Comisia a efectuat două revizuiți 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<sup>25</sup> la 29 ianuarie 2015. Comisia a adoptat, de asemenea, un catalog de bune practici și recomandări<sup>26</sup>. 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<sup>27</sup>, 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 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 minorilor dispăruți.

---

<sup>25</sup> 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).

<sup>26</sup> 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].

<sup>27</sup> 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).

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 prelucrez 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, inclusiv reducerea perioadelor de păstrare a semnalărilor privind obiecte. Se recunosc explicit și există dispoziții privind drepturile persoanelor de a accesa și a rectifica datele care le privesc și de a solicita ștergerea acestora în conformitate cu drepturile lor fundamentale (a se vedea secțiunea referitoare la protecția și securitatea datelor).

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. Identificarea mai fiabilă a persoanelor va fi posibilă prin utilizarea de date biometrice pentru persoanele dispărute care au nevoie de protecție, asigurându-se exactitatea și protecția corespunzătoare a datelor cu caracter personal. 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<sup>28</sup> din perspectiva dreptului la protecția datelor cu caracter personal. Dezvoltarea și menținerea eficacității SIS vor contribui la asigurarea securității persoanelor în cadrul societății.

Propunerea prevede modificări semnificative în ceea ce privește elementele biometrice de identificare. În plus față de amprente digitale, amprente palmare ar trebui, de asemenea, să fie colectate și stocate, dacă sunt îndeplinite cerințele legale. Fișierele amprentelor digitale sunt atașate la semnalările alfanumerice din SIS, astfel cum se prevede la articolele 26, 32, 34 și 36. 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 plus, propunerea prevede stocarea amprentelor digitale pentru așa-numitele „persoane căutate necunoscute” (condițiile sunt descrise în detaliu în secțiunea 5 subsecțiunea „Fotografii, imagini faciale, date dactiloscopice și profiluri ADN”). În caz de incertitudine în ceea ce

---

<sup>28</sup>

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

privește identitatea unei persoane pe baza documentelor sale, autoritățile competente ar trebui să verifice amprente 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 dintre propuneri [prezenta propunere și Propunerea de regulament privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere] 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 fișă 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<sup>29</sup>. 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

<sup>29</sup>

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.

sprijinului pentru frontiere<sup>30</sup> 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 71 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;
- 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 dispozițiile specifice ale propunerii**

#### **Dispoziții care sunt comune prezentei propuneri și Propunerii de regulament privind instituirea, funcționarea și utilizarea SIS în domeniul verificărilor la frontiere**

- dispozițiile generale (articolele 1-3);
- arhitectura tehnică a SIS și modul de funcționare a acestuia (articolele 4-14);

<sup>30</sup>

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).

- responsabilitățile eu-LISA (articolele 15-18);
- dreptul de acces la semnalări și păstrarea acestora (articolele 43, 46, 48, 50 și 51);
- normele generale de prelucrare a datelor și de protecție a datelor (articolele 53-70);
- monitorizare și statistici (articolul 71).

### **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, aceștia 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<sup>31</sup>.

### **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.

<sup>31</sup>

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).

## **Calitatea datelor**

Propunerea menține principiul conform căruia statul membru care este proprietarul datelor răspunde, de asemenea, de exactitatea datelor introduse în SIS (articolul 56). 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 71). 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 în 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 plus, modificările aduse articolului 22 și noile articole 40, 41 și 42 vor permite, pe lângă utilizarea amprentelor digitale, și utilizarea imaginilor faciale, a amprentelor palmare și a profilurilor ADN pentru a identifica o persoană. 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. Dactiloscopia este studiarea științifică a amprentelor digitale ca metodă de identificare. Experții în dactiloscopie recunosc faptul că amprente palmare se caracterizează prin unicitate și că acestea conțin puncte de referință care permit comparații fiabile și concludente, la fel ca și amprente digitale. Ampretele palmare se pot utiliza pentru stabilirea identității unei persoane în același mod ca și amprente 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. Există două utilizări principale ale amprentelor palmare:

- (i) în scopul identificării, atunci când persoana vizată și-a deteriorat în mod intenționat sau neintenționat vârful 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, Italia a declarat că a reușit astfel să identifice migranții în situație nereglementară care și-au deteriorat intenționat vârful degetelor, încercând în acest mod să evite identificarea. Prelevarea amprentelor palmare de către autoritățile italiene a permis identificarea ulterioară;
- (ii) amprente latente prelevate de la locul infracțiunilor. Adesea, persoana suspectată lasă urme la locul infracțiunii și se constată că acestea sunt urme palmare. Un suspect poate fi identificat doar dacă amprente palmare se prelevează în mod obișnuit atunci când o persoană este supusă în mod legal amprentării digitale. De asemenea, amprenta palmară conține de obicei detalii de la baza degetelor care adesea lipsesc din amprente prelevate prin apăsarea degetului de la un capăt al unghiei la celălalt și din amprente plane, deoarece acestea tind să se concentreze asupra vârfulor degetelor și a părții superioare a articulațiilor.

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.

În cazurile în care nu sunt disponibile amprente digitale sau amprente palmare, articolul 22 alineatul (1) litera (b) permite utilizarea profilurilor ADN pentru persoanele dispărute care trebuie plasate sub protecție, în special copii. Această funcționalitate va fi folosită doar în cazul în care nu sunt disponibile amprente digitale și va fi accesibilă numai utilizatorilor autorizați. Prin urmare, această dispoziție autorizează utilizarea profilurilor ADN ale părinților sau ale fraților ori surorilor persoanei dispărute/copilului dispărut pentru a permite autorităților naționale să o (îl) identifice. Statele membre își transmit deja aceste informații la nivel operațional, prin intermediul schimbului de informații suplimentare. Prezenta propunere înscrie această practică într-un cadru de reglementare, prin introducerea sa în temeiul juridic material al funcționării și al utilizării SIS și prin introducerea unor proceduri clare privind situațiile în care se pot utiliza aceste profiluri.

Modificările propuse vor permite, de asemenea, să se emită semnalări SIS privind persoane necunoscute căutate în legătură cu o infracțiune, pe baza amprentelor digitale sau a amprentelor palmare (articolele 40-42). Aceste semnalări pot fi create în cazul în care, de exemplu, la locul unei infracțiuni grave se descoperă amprente digitale sau amprente palmare latente și în cazul în care există motive întemeiate pentru a suspecta că amprente digitale aparțin autorului respectivei infracțiuni. De exemplu, atunci când amprente digitale sunt găsite pe o armă folosită la comiterea infracțiunii sau pe orice alt obiect utilizat de autor în momentul în care a comis infracțiunea. Această nouă categorie de semnalări completează dispozițiile Prüm care permit interconectarea sistemelor naționale de identificare a amprentelor digitale ale autorilor infracțiunilor. Prin intermediul mecanismului Prüm, un stat membru poate introduce o cerere pentru a verifica dacă autorul unei infracțiuni ale cărui amprente digitale au fost găsite este cunoscut în orice alt stat membru (de obicei în scopuri investigative). O persoană poate fi identificată prin intermediul mecanismului Prüm numai dacă i s-au prelevat amprente digitale în alt stat membru ca urmare a comiterii unei infracțiuni. Prin urmare, infractorii fără antecedente nu pot fi identificați. Dezvoltările prevăzute în prezenta propunere, și anume stocarea amprentelor digitale ale persoanelor căutate necunoscute, vor permite ca amprente digitale ale unui autor necunoscut să fie încărcate în SIS, astfel încât acesta să poată fi identificat ca fiind căutat dacă este găsit în alt stat membru. Utilizarea acestei funcționalități presupune că statele membre au efectuat în prealabil o consultare a tuturor surselor naționale și internaționale disponibile, dar nu au putut stabili identitatea persoanei vizate. Propunerea conține garanții suficiente pentru a se asigura faptul că în SIS sunt stocate în cadrul acestei categorii doar amprente digitale ale persoanelor în privința cărora există suspiciuni puternice că au comis o infracțiune gravă sau o infracțiune de terorism. În consecință, se permite recurgerea la această nouă categorie de semnalări numai în cazurile în care autorul necunoscut reprezintă un risc major pentru siguranța publică, justificându-se astfel compararea acestor amprente cu amprente digitale ale călătorilor, de exemplu pentru a se evita ca respectiva persoană să părăsească spațiul fără controale la frontierele interne.

Dispoziția menționată nu permite utilizatorilor finali să introducă amprente digitale în cadrul acestei categorii în cazul în care nu se poate stabili o legătură între respectivele amprente digitale și autor. O altă condiție va fi aceea că identitatea persoanei nu poate fi stabilită prin utilizarea niciunei alte baze de date naționale, europene sau internaționale în care sunt stocate amprente digitale. Odată stocate în SIS, aceste amprente digitale vor fi utilizate pentru identificarea persoanelor a căror identitate nu poate fi stabilită în alte moduri. În cazul în care în urma efectuării de căutări în date se identifică o potențială corespondență (*match*), statul membru ar trebui să efectueze verificări suplimentare ale respectivelor amprente digitale, eventual cu ajutorul experților din domeniul dactiloscopic, pentru a determina dacă amprente stocate în SIS aparțin respectivei persoane și ar trebui să stabilească identitatea acesteia. Procedurile sunt reglementate de dreptul național. O identificare în SIS a unei

„persoane căutate necunoscute” ca fiind persoana căreia îi aparțin respectivele amprente poate duce la arestare.

### **Accesul la SIS**

Această subsecțiune descrie elementele noi în ceea ce privește drepturile de acces la SIS ale autorităților naționale competente, precum și ale agențiilor UE (utilizatorii instituționali).

### **Autoritățile naționale - autoritățile din domeniul imigrației**

Pentru a se asigura cea mai eficace utilizare a SIS, propunerea acordă acces la SIS autorităților naționale responsabile cu examinarea condițiilor și luarea deciziilor privind intrarea, șederea și returnarea resortisanților țărilor terțe pe teritoriul statelor membre. Această adăugare permite consultarea SIS în cazul migranților în situație neregulamentară care nu au făcut la frontieră obiectul unor controale obișnuite. Această propunere asigură egalitatea de tratament a resortisanților țărilor terțe care trec frontierele externe la punctele obișnuite de trecere a frontierei (și care, prin urmare, fac obiectul verificărilor aplicabile resortisanților țărilor terțe) și a resortisanților țărilor terțe care sosesc neregulamentar în spațiul Schengen.

În plus, prezenta propunere asigură faptul că autoritățile de înmatriculare a vehiculelor (articolul 44), a ambarcațiunilor și a aeronavelor vor avea un acces limitat la sistem pentru a-și îndeplini sarcinile, cu condiția ca respectivele autorități să fie servicii publice. Acest lucru va contribui la evitarea înregistrării mijloacelor de transport menționate dacă sunt furate și căutate în alte state membre. În ceea ce privește serviciile de înmatriculare a vehiculelor, inițiativa nu este nouă, deoarece accesul acestora la SIS a fost deja prevăzut la articolul 102a din Convenția Schengen și în Regulamentul (CE) nr. 1986/2006<sup>32</sup>. Urmând aceeași logică, propunerea prevede accesul autorităților de înmatriculare a ambarcațiunilor și a aeronavelor la semnalările din SIS privind ambarcațiuni și aeronave.

### **Utilizatorii instituționali**

Europol (articolul 46), Eurojust (articolul 47) 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 (articolele 48 și 49) 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 50, 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 persoane dispărute, ceea ce asigură faptul că acesta poate utiliza în mod optim sistemul pentru îndeplinirea atribuțiilor 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. În cadrul lucrărilor Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate și în scopul de a îmbunătăți și mai mult schimbul de informații privind terorismul, Comisia va evalua dacă Europol ar trebui să primească în mod automat o notificare din partea SIS atunci când se creează o semnalare privind activități legate de terorism.

<sup>32</sup>

Regulamentul (CE) nr. 1986/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind accesul la Sistemul de Informații Schengen din a doua generație (SIS II) al serviciilor competente, în statele membre, pentru eliberarea certificatelor de înmatriculare a vehiculelor (JO L 381, 28.12.2006, p. 1).

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)<sup>33</sup>, unitatea centrală a ETIAS din cadrul Agenției Europene pentru Poliția de Frontieră și Garda de Coastă va efectua căutări în SIS prin intermediul ETIAS pentru a verifica 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 deplin la SIS.

### **Modificări specifice privind semnalările**

Articolul 26 oferă statelor membre posibilitatea de a suspenda temporar semnalările în vederea arestării (în cazul unei operațiuni de poliție sau al unei investigații în curs), astfel încât pentru o perioadă limitată de timp acestea să fie vizibile doar pentru birourile SIRENE, însă nu și pentru agenții de pe teren. Această dispoziție contribuie la evitarea situației în care o operațiune de poliție confidențială în scopul arestării unui infractor foarte căutat este pusă în pericol de un agent de poliție care nu este implicat în respectiva operațiune.

Articolele 32 și 33 cuprind dispoziții referitoare la semnalările privind persoane dispărute. Modificările aduse acestora permit emiterea de semnalări preventive în cazurile în care există un risc ridicat de răpire de către unul dintre părinți și prevăd o împărțire pe categorii mai bine ajustată a semnalărilor privind persoane dispărute. Răpirea de către unul dintre părinți este adesea minuțios planificată, cu intenția de a părăsi rapid teritoriul statului membru în care s-a convenit asupra condițiilor încredințării. Modificările remediază o potențială lacună în legislația actuală care prevede că semnalările privind copiii pot fi emise numai după dispariția acestora. Modificările vor permite autorităților din statele membre să menționeze copii care sunt expuși unui risc deosebit. Aceste modificări vor însemna că, în cazul în care există un risc ridicat de răpire iminentă de către unul dintre părinți, polițiștii de frontieră și agenții de asigurare a respectării legii sunt informați cu privire la risc și vor putea să analizeze mai îndeaproape circumstanțele în care călătorește un copil aflat în situație de risc, plasându-l într-un serviciu de protecție, dacă este necesar. Prin intermediul birourilor SIRENE se vor furniza informații suplimentare, inclusiv privind decizia autorității judiciare competente care a solicitat emiterea semnalării. Manualul SIRENE va fi revizuit în consecință. Pentru emiterea acestei semnalări va fi necesar să existe o decizie corespunzătoare a autorităților judiciare prin care copilul este încredințat unui singur părinte. O altă condiție va fi existența unui risc iminent de răpire. Statutul semnalărilor privind copiii dispăruți se va actualiza în mod automat pentru a reflecta împlinirea vârstei majoratului, dacă este cazul.

Articolul 34 permite ca unei semnalări să i se adauge date privind vehicule, dacă există indicii clare că acestea au legătură cu persoana căutată.

Articolul 37 introduce o nouă formă de verificare, „verificarea prin interviu”. Aceasta este menită, în special, să sprijine măsurile de combatere a terorismului și a infracțiunilor grave și permite autorităților să oprească și să interogheze persoana vizată. Este o verificare mai aprofundată decât controlul discret existent, dar nu implică percheziționarea persoanei și nu duce la arestarea acesteia. Această verificare poate însă să furnizeze suficiente informații pentru a decide cu privire la întreprinderea de acțiuni suplimentare. Se modifică, de asemenea, articolul 36 pentru a reflecta acest nou tip de verificare.

Prezenta propunere prevede introducerea de semnalări în SIS pentru documente oficiale în alb și documente de identitate eliberate (articolul 36) și vehicule, inclusiv ambarcațiuni și aeronave (articolele 32 și 34), în cazul în care acestea au legătură cu semnalări privind persoane emise în temeiul acestor articole. Se modifică articolul 37 pentru a stabili acțiunea

care trebuie întreprinsă pe baza acestor semnalări. Obiectivul vizat este pur investigativ, deoarece va permite autorităților să gestioneze situațiile în care mai multe persoane folosesc documente autentice asemănătoare, dar nu sunt titularii legali ai acestora.

La articolul 38 se stabilește o listă extinsă de obiecte în cazul cărora se pot emite semnalări, adăugându-se documentele falsificate, vehiculele, indiferent de sistemul de propulsie (și anume electrice, care utilizează benzină sau motorină etc.), bancnotele falsificate, echipamentele informatice, componentele identificabile ale vehiculelor și echipamentele industriale. La articolul menționat nu mai sunt prevăzute semnalările privind mijloacele de plată, deoarece acestea au avut o eficiență foarte scăzută și nu au generat suficiente rezultate pozitive.

În vederea clarificării procedurii care trebuie urmată după găsirea unui obiect în privința căruia s-a emis o semnalare, articolul 39 a fost modificat pentru a se preciza faptul că obiectele trebuie confiscate, în conformitate cu dreptul național, pe lângă contactarea autorității care a emis semnalarea.

### **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 57).

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

Articolul 12 include, de asemenea, dispoziții privind căutările automate prin scanarea plăcuțelor de înmatriculare a autovehiculelor, prin utilizarea sistemelor de recunoaștere automată a numărului de înmatriculare, și impune statelor membre obligația de a păstra înregistrările acestor căutări în conformitate cu dreptul național.

Articolul 15 alineatul (3) menține dispozițiile articolului 15 alineatul (3) din Decizia 2007/533/JAI a Consiliului și prevede că Comisia rămâne responsabilă cu gestionarea contractelor aferente infrastructurii de comunicare, inclusiv 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 de a analiza dacă un caz este suficient de adecvat, de relevant și de important, aceasta aplicându-se și deciziilor prin care se stabilește dacă perioada de valabilitate a unei semnalări ar trebui să fie prelungită. Ca element de noutate, acest articol prevede, de asemenea, obligația statelor membre de a crea în toate circumstanțele o semnalare prevăzută la articolele 34, 36 și 38 (după caz) care să vizeze persoane a căror activitate intră sub incidența articolelor 1, 2, 3 și 4 din Decizia-cadru 2002/475/JAI a Consiliului privind combaterea terorismului sau o semnalare care să vizeze obiecte care au legătură cu respectivele persoane.

### **Categoriile de date și prelucrarea datelor**

Prezenta propunere extinde tipurile de informații (articolul 20) care pot fi deținute referitor la persoanele în privința cărora s-a emis o semnalare, astfel încât printre aceste informații să se numere și următoarele elemente:

- dacă persoana vizată este implicată în orice activitate care intră sub incidența articolelor 1, 2, 3 și 4 din Decizia-cadru 2002/475/JAI a Consiliului;
- alte observații privind persoana vizată; motivul semnalării;
- informații privind numărul național de înregistrare al persoanei vizate și locul de înregistrare al acesteia;

- clasificarea tipului de caz de persoană dispărută (doar pentru semnalările prevăzute la articolul 32);
- detalii privind documentul de identitate sau de călătorie al persoanei vizate;
- o copie color a documentului de identitate sau de călătorie al persoanei vizate;
- profiluri ADN (numai dacă nu sunt disponibile amprente digitale care să permită identificarea).

Articolul 59 extinde lista datelor cu caracter personal care pot fi introduse și prelucrate în SIS în scopul tratării cazurilor de identitate uzurpată. Aceste date pot fi introduse numai cu acordul victimei căreia i s-a uzurpat identitatea. 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, include detalii privind documentele de identificare personale ale persoanelor vizate și permite clasificarea în categorii a cazurilor de copii dispăruți în funcție de circumstanțele dispariției acestora, cum ar fi „minori neînsoțiți”, „răpire de către unul dintre părinți”, „fugă” etc. Acest lucru este esențial pentru ca utilizatorii finali să ia de îndată măsurile necesare în vederea protecției copiilor în cauză. 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<sup>34</sup>.

Propunerea clarifică faptul că statele membre nu trebuie să copieze datele introduse de un alt stat membru în alte fișiere de date naționale (articolul 53).

#### Păstrarea

Perioada maximă de păstrare a unei semnalări privind persoane va fi prelungită la cinci ani, cu excepția semnalărilor în vederea efectuării de controale discrete, de verificări prin interviu sau de controale specifice, în cazul cărora perioada de păstrare rămâne de un an. Statele membre pot stabili întotdeauna perioade de valabilitate mai scurte. Perioada maximă extinsă de valabilitate urmează practicile naționale de a prelungi termenul de expirare a valabilității unei semnalări dacă aceasta nu și-a atins încă obiectivul și persoana vizată este în continuare căutată. În plus, era necesar să se alinieze SIS la perioada de păstrare prevăzută de alte instrumente, cum ar fi Directiva privind returnarea și Eurodac. Din motive de transparență și de claritate, este necesar să se prevadă aceeași perioadă de păstrare pentru semnalările privind persoane, cu excepția semnalărilor create în vederea efectuării de controale discrete, de verificări prin interviu sau de controale specifice. Prolungirea perioadei de păstrare nu pune în pericol interesul persoanelor vizate, deoarece o semnalare nu poate fi păstrată mai mult timp

<sup>34</sup>

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

decât este necesar pentru scopul său. Normele privind ștergerea unei semnalări sunt stabilite în mod explicit la articolul 52. Articolul 51 stabilește termenul de reexaminare a semnalărilor și prevede, în special, o reducere a perioadei de păstrare a semnalărilor privind obiecte. În absența unei nevoi operaționale care să justifice păstrarea pentru o perioadă mai îndelungată a semnalărilor privind obiecte, termenul de păstrare al acestora fost redus la cinci ani, în vederea alinierii sale la perioada de păstrare a semnalărilor privind persoane. Termenul de expirare a valabilității semnalărilor privind documente eliberate și în alb rămâne însă de 10 ani, deoarece perioada de valabilitate a documentelor este de 10 ani.

### Ștergerea

Articolul 52 stabilește circumstanțele în care semnalările trebuie șterse, ceea ce duce la o armonizare sporită a practicilor naționale din acest domeniu. Articolul 51 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<sup>35</sup> și cu Directiva 2016/680<sup>36</sup>. În plus, articolul 63 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.

Schimbul de date cu Interpol privind documentele de călătorie furate, însușite în mod ilegal, pierdute și anulate

Articolul 63 păstrează în totalitate articolul 55 din Decizia 2007/533/JAI a Consiliului, deoarece chestiunea îmbunătățirii interoperabilității dintre secțiunea „Documente” a SIS și baza de date a Interpol privind documente pierdute și furate va fi abordată în comunicarea Grupului de experți la nivel înalt și în al doilea set de propuneri privind SIS, în iunie 2017.

### Statistici

Pentru a menține o imagine de ansamblu asupra modului de funcționare în practică a căilor de atac, articolul 66 prevede un sistem statistic standard care să furnizeze rapoarte anuale 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;
- cauze în care o instanță judecătorească s-a pronunțat în favoarea reclamantului și

---

<sup>35</sup> 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).

<sup>36</sup> 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).

- 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 71 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 71 alineatul (5) prevede obligația eu-LISA de a furniza statelor membre, Comisiei, Europol, Eurojust 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 71 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, Eurojust și Agenției Europene pentru Poliția de Frontieră și Garda de Coastă să aibă acces la datele enumerate la articolul 71 alineatul (3) în vederea întocmirii statisticilor necesare.

Propunere de

**REGULAMENT 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, de modificare a Regulamentului (UE) nr. 515/2014 și de abrogare a Regulamentului (CE) nr. 1986/2006, a Deciziei 2007/533/JAI a Consiliului și a Deciziei 2010/261/UE a Comisiei**

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 82 alineatul (1) al doilea paragraf litera (d), articolul 85 alineatul (1), articolul 87 alineatul (2) litera (a) și articolul 88 alineatul (2) litera (a),

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 și autoritățile judiciare în materie penală.
- (2) SIS a fost înființat 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<sup>37</sup> (Convenția Schengen). Dezvoltarea SIS de a doua generație (SIS II) a fost încredințată Comisiei în temeiul Regulamentului (CE) nr. 2424/2001 al Consiliului<sup>38</sup> și al Deciziei 2001/886/JAI a Consiliului<sup>39</sup> și acest sistem a fost instituit prin Regulamentul (CE) nr.

<sup>37</sup> 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).

<sup>38</sup> JO L 328, 13.12.2001, p. 4.

<sup>39</sup> 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).

1987/2006<sup>40</sup>, precum și prin Decizia 2007/533/JAI a Consiliului<sup>41</sup>. SIS II a înlocuit SIS, astfel cum a fost creat în temeiul Convenției Schengen.

- (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 conexe au fost adoptate la 21 decembrie 2016<sup>42</sup>. 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 capitolele 4 și 5 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 verificărilor la frontiere<sup>43</sup> 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.
- (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.

---

<sup>40</sup> 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).

<sup>41</sup> 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).

<sup>42</sup> 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...).

<sup>43</sup> Regulamentul (UE) 2018/...

- (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.
- (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<sup>44</sup> („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 în materie de infracțiuni, 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, pentru a facilita identificarea persoanelor și pentru a depista identitățile multiple, categoriile de date privind persoane 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 inconveniente 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

<sup>44</sup>

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).

Parlamentului European și a Consiliului<sup>45</sup>. Acest lucru ar trebui să asigure că SIS 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 amprentelor digitale 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) Introducerea unui sistem automat de identificare a amprentelor digitale în cadrul SIS completează mecanismul Prüm existent privind accesul online transfrontalier reciproc la bazele de date ADN și sistemele automate de identificare a amprentelor digitale naționale desemnate<sup>46</sup>. Mecanismul Prüm permite interconectarea sistemelor naționale de identificare a amprentelor digitale, un stat membru putând astfel să introducă o cerere pentru a verifica dacă autorul unei infracțiuni ale cărei amprente digitale au fost găsite este cunoscut în orice alt stat membru. Mecanismul Prüm verifică doar dacă persoana căreia îi aparțin respectivele amprente digitale este cunoscută la un anumit moment, prin urmare, dacă autorul este cunoscut ulterior în oricare dintre statele membre, nu va fi în mod necesar reținut. Verificarea în SIS a amprentelor digitale permite o căutare activă a autorului. Prin urmare, ar trebui să fie posibil să se încarce în SIS amprente digitale ale unui autor necunoscut, cu condiția ca persoana căreia îi aparțin respectivele amprente digitale să poată fi identificată cu un grad ridicat de probabilitate ca autor al unei infracțiuni grave sau al unui act de terorism. Acest lucru este valabil în special în cazul în care amprente digitale sunt găsite pe o armă sau pe orice obiect utilizat la comiterea infracțiunii. Simpla prezență a amprentelor digitale la locul infracțiunii nu ar trebui considerată ca indicând cu un grad ridicat de probabilitate că amprente digitale aparțin autorului. O altă condiție prealabilă pentru crearea unei astfel de semnalări ar trebui să fie aceea ca identitatea autorului să nu poată fi stabilită prin intermediul niciunei alte baze de date naționale, europene sau internaționale. În cazul în care în urma efectuării de căutări în date se identifică o potențială corespondență, statul membru ar trebui să efectueze verificări suplimentare ale respectivelor amprente digitale, eventual cu ajutorul experților din domeniul dactiloscopic, pentru a determina dacă amprente stocate în SIS aparțin respectivei persoane și ar trebui să stabilească identitatea acesteia. Procedurile ar trebui să fie reglementate de dreptul național. O identificare în SIS a unei „persoane căutate necunoscute” ca fiind persoana căreia îi aparțin respectivele amprente digitale poate

<sup>45</sup> Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

<sup>46</sup> Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008, p. 1) și Decizia 2008/616/JAI a Consiliului din 23 iunie 2008 privind punerea în aplicare a Deciziei 2008/615/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008, p.12).

contribui în mod substanțial la investigație și poate conduce la arestare, sub rezerva îndeplinirii tuturor condițiilor în vederea arestării.

- (19) Ampretele digitale găsite la locul unei infracțiuni ar trebui să poată fi verificate prin consultarea amprentelor digitale 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<sup>47</sup> și „infracțiune de terorism” ar trebui să fie infracțiunile prevăzute de dreptul național menționate în Decizia-cadru 2002/475/JAI a Consiliului<sup>48</sup>.
- (20) Ar trebui să fie posibil să se adauge un profil ADN în cazurile în care datele dactiloscopice nu sunt disponibile, iar acesta ar trebui să fie accesibil doar utilizatorilor autorizați. Profilurile ADN ar trebui să faciliteze identificarea persoanelor dispărute care au nevoie de protecție, în special a copiilor dispăruți, inclusiv prin autorizarea utilizării profilurilor ADN ale părinților sau ale fraților ori surorilor pentru a se putea efectua identificarea. Datele ADN nu ar trebui să conțină trimiteri la originea rasială.
- (21) SIS ar trebui să conțină semnalări privind persoane căutate în vederea arestării în scopul predării și al extrădării. În afară de semnalări, este oportun să se asigure schimbul de informații suplimentare care sunt necesare pentru procedurile de predare și de extrădare. În special, în SIS ar trebui să se prelucreze datele menționate la articolul 8 din Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre<sup>49</sup>. Din motive operaționale, este oportun ca statul membru semnalant, cu autorizația autorităților judiciare, să suspende temporar disponibilitatea unei semnalări în vederea arestării atunci când o persoană care face obiectul unui mandat european de arestare este căutată în mod intens și activ și utilizatorii finali care nu sunt implicați în operațiunea de căutare concretă pot pune în pericol succesul acesteia. Indisponibilitatea temporară a acestor semnalări nu ar trebui să depășească 48 de ore.
- (22) Ar trebui să fie posibil să se adauge în SIS o traducere a datelor suplimentare introduse în scopul predării în temeiul mandatului european de arestare și în scopul extrădării.
- (23) SIS ar trebui să conțină semnalări privind persoane dispărute pentru a se asigura protecția acestora sau pentru a se preveni amenințările la adresa siguranței publice. Ar trebui să se limiteze emiterea în SIS a semnalărilor privind copiii expuși riscului de răpire (și anume pentru a preveni un prejudiciu viitor care nu s-a produs încă, așa cum este cazul copiilor expuși riscului de a fi răpiți de către unul dintre părinți), prin urmare este oportun să se prevadă garanții stricte și corespunzătoare. În cazul copiilor, aceste semnalări și procedurile corespunzătoare ar trebui să servească interesul superior al copilului, având în vedere articolul 24 din Carta drepturilor fundamentale a Uniunii Europene și Convenția Organizației Națiunilor Unite cu privire la drepturile copilului din 20 noiembrie 1989.
- (24) Pentru cazurile în care există suspiciuni legate de terorism și de infracțiuni grave, ar trebui să se includă o nouă acțiune care să permită oprirea și interogarea unei persoane care este suspectată că a comis o infracțiune gravă sau în cazul în care există motive să

---

<sup>47</sup> 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).

<sup>48</sup> Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO L 164, 22.6.2002, p. 3).

<sup>49</sup> 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).

se creadă că respectiva persoană va comite o infracțiune gravă, în scopul de a furniza informații cât mai detaliate posibil statului membru semnalant. Această nouă acțiune nu ar trebui să implice nici percheziționarea, nici arestarea respectivei persoane. Totuși, aceasta ar trebui să furnizeze suficiente informații pentru a se decide cu privire la întreprinderea de acțiuni suplimentare. Infracțiunile grave ar trebui să fie infracțiunile enumerate în Decizia-cadru 2002/584/JAI a Consiliului.

- (25) SIS ar trebui să conțină noi categorii de obiecte de valoare ridicată, cum ar fi echipamentele electronice și tehnice care pot fi identificate și care pot face obiectul unei căutări cu ajutorul unui număr unic.
- (26) Ar trebui să fie posibil ca un stat membru să aplice unei semnalări o mențiune, denumită „indicator de validitate”, care să arate că acțiunea care trebuie întreprinsă pe baza semnalării nu va fi întreprinsă pe teritoriul său. În cazul în care semnalările sunt emise în vederea arestării în scopul predării, nicio dispoziție a prezentului regulament nu ar trebui interpretată pentru a deroga de la dispozițiile Deciziei-cadru 2002/584/JAI sau pentru a împiedica aplicarea acestora. Decizia de a adăuga un indicator de validitate unei semnalări ar trebui să se bazeze numai pe motivele de refuz prevăzute în decizia-cadru menționată.
- (27) În cazul în care s-a adăugat un indicator de validitate și se identifică locul în care se află persoana căutată pentru a fi arestată în vederea predării, acest loc ar trebui comunicat întotdeauna autorității judiciare semnalante, care poate decide transmiterea unui mandat european de arestare autorității judiciare competente în conformitate cu dispozițiile Deciziei-cadru 2002/584/JAI.
- (28) 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.
- (29) 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 diversele autorități implicate în prelucrarea datelor privind persoane în diferite scopuri, este oportun să se alinieze perioada de păstrare a semnalărilor privind persoane la perioadele de păstrare prevăzute pentru returnare și cazurile de ședere ilegală. În plus, statele membre extind periodic termenul de expirare a valabilității semnalărilor privind persoane dacă acțiunea necesară nu a putut fi întreprinsă în perioada prevăzută inițial. Prin urmare, perioada de păstrare a semnalărilor privind persoane ar trebui să fie de maximum cinci ani. Ca principiu general, semnalările privind persoane ar trebui șterse în mod automat din SIS după o perioadă de cinci ani, cu excepția semnalărilor emise în scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice. Acestea ar trebui șterse după un an. Semnalările privind obiecte introduse în scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice ar trebui șterse în mod automat din SIS după o perioadă de un an, deoarece acestea au legătură întotdeauna cu persoane. Semnalările privind obiecte căutate pentru a fi confiscate sau folosite ca probe în cadrul procedurilor penale ar trebui să fie șterse în mod automat din SIS după cinci ani, deoarece după scurgerea acestei perioade probabilitatea de a găsi obiectele respective este foarte redusă și valoarea lor economică a scăzut în mod semnificativ. Semnalările privind documente de identificare eliberate și în alb ar trebui păstrate timp de 10 ani, deoarece perioada de valabilitate a documentelor este de 10 ani de la data eliberării. 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.

- (30) 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. Infracțiunile prevăzute la articolele 1, 2, 3 și 4 din Decizia-cadru 2002/475/JAI a Consiliului privind combaterea terorismului<sup>50</sup> reprezintă o amenințare foarte gravă la adresa siguranței publice și a integrității vieții persoanelor și la adresa societății, iar aceste infracțiuni sunt extrem de dificil de prevenit, de depistat și de investigat într-un spațiu fără controale la frontierele interne în care potențialii infractori circulă liber. În cazul în care se caută o persoană sau un obiect în legătură cu aceste infracțiuni, este întotdeauna necesar să se creeze în SIS o semnalare corespunzătoare privind persoane căutate în vederea participării la o procedură judiciară penală, privind persoane sau obiecte care fac obiectul unor controale discrete, al unor verificări prin interviu sau al unor controale specifice, precum și privind obiecte căutate în vederea confiscării, deoarece niciun alt mijloc nu ar fi la fel de eficace în acest scop.
- (31) Este necesar să se prevadă dispoziții clare în ceea ce privește ștergerea semnalărilor. O semnalare ar trebui să fie păstrată numai pe durata perioadei necesare îndeplinirii scopului pentru care a fost introdusă. Având în vedere practicile divergente ale statelor membre privind definirea momentului în care o semnalare își îndeplinește scopul, este oportun să se prevadă criterii detaliate pentru fiecare categorie de semnalări în scopul de a stabili momentul în care acestea ar trebui să fie șterse din SIS.
- (32) 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.
- (33) 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. Cu toate acestea, este oportun să se consolideze cooperarea dintre Uniunea Europeană și Interpol prin promovarea unui schimb eficient de date privind pașapoartele. În cazul în care se transferă din SIS către Interpol date cu caracter personal, acestea ar trebui să beneficieze de un nivel de protecție adecvat, asigurat printr-un acord, care să prevadă garanții și condiții stricte.
- (34) Este oportun să se acorde acces la SIS autorităților responsabile cu înmatricularea vehiculelor, a ambarcațiunilor și a aeronavelor pentru ca acestea să poată verifica dacă mijlocul de transport este căutat deja într-un stat membru în scopul de a fi confiscat sau de a face obiectul unei verificări. Autorităților care sunt servicii publice ar trebui să li se acorde un acces direct. Acest acces ar trebui să se limiteze la semnalările privind respectivele mijloace de transport și certificatul sau plăcuța lor de înmatriculare. În consecință, dispozițiile Regulamentului (CE) nr. 1986/2006 al

<sup>50</sup>

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

Parlamentului European și al Consiliului<sup>51</sup> ar trebui să fie incluse în prezentul regulament și regulamentul menționat ar trebui abrogat.

- (35) În ceea ce privește prelucrarea datelor de către autoritățile naționale competente în scopul prevenirii, al investigării și al depistării infracțiunilor grave sau al infracțiunilor de terorism ori al urmăririi penale a infracțiunilor și al executării pedepselor penale, inclusiv garanțiile de asigurare a prevenirii amenințărilor la adresa siguranței publice, ar trebui să se aplice dispozițiile naționale de transpunere a Directivei (UE) 2016/680. Dispozițiile Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului<sup>52</sup> și ale Directivei (UE) 2016/680 ar trebui să fie detaliate în prezentul regulament, dacă este necesar.
- (36) Regulamentul (UE) 2016/679 ar trebui să se aplice prelucrării datelor cu caracter personal în temeiul prezentului regulament de către autoritățile naționale atunci când nu se aplică Directiva (UE) 2016/680. Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului<sup>53</sup> 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.
- (37) 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<sup>54</sup> (Regulamentul privind Europol).
- (38) În cazul prelucrării datelor din SIS de către Eurojust se aplică dispozițiile privind protecția datelor prevăzute în Decizia 2002/187/JAI din 28 februarie 2002 de instituire a Eurojust în scopul consolidării luptei împotriva formelor grave de criminalitate<sup>55</sup>, inclusiv cele privind competențele Organismului comun de supraveghere, înființat în temeiul deciziei menționate, de a monitoriza activitățile Eurojust și cele privind răspunderea pentru orice prelucrare ilegală a datelor cu caracter personal de către Eurojust. În cazurile în care căutările efectuate în SIS de Eurojust indică existența unei semnalări emise de un stat membru, Eurojust nu poate întreprinde acțiunea necesară. Prin urmare, acesta ar trebui să informeze statul membru în cauză care să îl autorizeze să se ocupe de caz.

---

<sup>51</sup> Regulamentul (CE) nr. 1986/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind accesul la Sistemul de Informații Schengen din a doua generație (SIS II) al serviciilor competente, în statele membre, pentru eliberarea certificatelor de înmatriculare a vehiculelor (JO L 381, 28.12.2006, p. 1).

<sup>52</sup> 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).

<sup>53</sup> 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).

<sup>54</sup> 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).

<sup>55</sup> Decizia 2002/187/JAI a Consiliului din 28 februarie 2002 de instituire a Eurojust în scopul consolidării luptei împotriva formelor grave de criminalitate (JO L 63, 6.3.2002, p. 1).

- (39) 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.
- (40) 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.
- (41) 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.
- (42) 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.
- (43) 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 grave de criminalitate și furnizează analize și evaluări ale amenințărilor. Extinderea drepturilor de acces ale Europol la semnalările din SIS privind persoane dispărute ar trebui să îmbunătățească și mai mult capacitatea acestuia de a furniza autorităților naționale de asigurare a respectării legii produse operaționale și analitice cuprinzătoare privind traficul de persoane și exploatarea sexuală a copiilor, inclusiv în mediul online. Extinderea ar contribui la o mai bună prevenire a acestor infracțiuni, la protecția potențialelor victime și la investigarea autorilor. Centrul european de combatere a criminalității informatice din cadrul Europol ar beneficia, de asemenea, de noul acces al Europol la semnalările din SIS privind persoane dispărute, inclusiv în cazurile delincvențelor sexuale itineranți și în cele de abuz sexual asupra copiilor pe internet în care autorii susțin adeseori că au acces sau pot avea acces la copii care ar putea să fi fost înregistrați ca dispăruți. În plus, având în vedere că Centrul european privind introducerea ilegală de migranți din cadrul Europol joacă un rol strategic fundamental în combaterea facilitării migrației neregulamentare, acesta ar trebui să obțină acces la semnalările privind persoanele cărora li s-a refuzat intrarea sau șederea pe teritoriul unui stat membru din motive ce țin de dreptul penal sau din cauza nerespectării condițiilor de acordare a vizei și de ședere.
- (44) 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.

- (45) 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.
- (46) Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului<sup>56</sup> 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 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.
- (47) 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)<sup>57</sup>, 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

<sup>56</sup> 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).

<sup>57</sup> COM (2016) 731 final.

din cadrul Agenției Europene pentru Poliția de Frontieră și Garda de Coastă ar trebui, de asemenea, să aibă acces la SIS în măsura necesară pentru îndeplinirea mandatului său, și anume la toate categoriile de semnalări privind persoane și la semnalările privind documente de identificare personale în alb sau eliberate.

- (48) 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, ștergerea 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, specificarea noilor categorii de obiecte din cadrul categoriei echipamentelor tehnice și electronice, stabilirea datei de expirare a valabilității semnalărilor în limitele termenului 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.
- (49) 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 trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011<sup>58</sup>. Procedura de adoptare a măsurilor de punere în aplicare prevăzute în prezentul regulament și în Regulamentul (UE) 2018/xxx (verificări la frontiere) ar trebui să fie aceeași.
- (50) 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.
- (51) 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.
- (52) 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 o protecție specială pentru copiii care ar putea cădea victimă traficului de persoane sau răpirii de către unul dintre părinți, respectând în același timp pe deplin protecția datelor cu caracter personal.
- (53) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu participă la adoptarea prezentului regulament, nu are obligații în temeiul acestuia și nu face obiectul aplicării sale. Deoarece prezentul regulament constituie o dezvoltare a acquis-ului Schengen, Danemarca decide, în

<sup>58</sup>

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).

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 internă.

- (54) Regatul Unit participă la prezentul regulament în conformitate cu articolul 5 din Protocolul privind acquis-ul Schengen integrat în cadrul Uniunii Europene, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, și în conformitate cu articolul 8 alineatul (2) din Decizia 2000/365/CE a Consiliului din 29 mai 2000 privind cererea Regatului Unit al Marii Britanii și Irlandei de Nord de a participa la punerea în aplicare a unora dintre dispozițiile acquis-ului Schengen<sup>59</sup>.
- (55) Irlanda participă la prezentul regulament în conformitate cu articolul 5 din Protocolul privind acquis-ul Schengen integrat în cadrul Uniunii Europene, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, și în conformitate cu articolul 6 alineatul (2) din Decizia 2002/192/CE a Consiliului din 28 februarie 2002 privind cererea Irlandei de a participa la unele dintre dispozițiile acquis-ului Schengen<sup>60</sup>.
- (56) 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 urmă la implementarea, aplicarea și dezvoltarea acquis-ului Schengen<sup>61</sup>, care intră sub incidența domeniului menționat la articolul 1 punctul G din Decizia 1999/437/CE a Consiliului<sup>62</sup> privind anumite modalități de aplicare a acordului menționat.
- (57) 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<sup>63</sup> și 2004/860/CE<sup>64</sup> ale Consiliului.
- (58) 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<sup>65</sup>, care intră sub incidența domeniului menționat la articolul 1 punctul G din Decizia

---

<sup>59</sup> JO L 131, 1.6.2000, p. 43.

<sup>60</sup> JO L 64, 7.3.2002, p. 20.

<sup>61</sup> JO L 176, 10.7.1999, p. 36.

<sup>62</sup> JO L 176, 10.7.1999, p. 31.

<sup>63</sup> 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).

<sup>64</sup> 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).

<sup>65</sup> JO L 160, 18.6.2011, p. 21.

1999/437/CE, coroborat cu articolul 3 din Decizia 2011/349/UE a Consiliului<sup>66</sup> și cu articolul 3 din Decizia 2011/350/UE a Consiliului<sup>67</sup>.

- (59) 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<sup>68</sup>.
- (60) 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 alineatul (2) din Actul de aderare din 2003 și, respectiv, al articolului 4 alineatul (2) din Actul de aderare din 2011.
- (61) Prezentul regulament ar trebui să se aplice Irlandei la date hotărâte în conformitate cu procedurile stabilite în instrumentele relevante privind aplicarea acquis-ului Schengen în acest stat.
- (62) 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<sup>69</sup>. 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.
- (63) Prin urmare, Decizia 2007/533/JAI a Consiliului și Decizia 2010/261/UE a Comisiei<sup>70</sup> ar trebui abrogate.
- (64) 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 ...

---

<sup>66</sup> 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).

<sup>67</sup> 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).

<sup>68</sup> JO L 166, 1.7.2010, p. 17.

<sup>69</sup> 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).

<sup>70</sup> 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).

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 capitolele 4 și 5 din Tratatul privind funcționarea Uniunii Europene referitoare la circulația persoanelor pe teritoriul acestora, 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 persoane și obiecte, precum și la schimbul de informații suplimentare și date suplimentare în scopul cooperării judiciare și polițienești în materie penală.
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 articolele 22 și 40, 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) „date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoană vizată”);
- (e) „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;
- (f) „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;
- (g) „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) sunt necesare acțiuni suplimentare;
- (h) „indicator de validitate” (*flag*) înseamnă suspendarea validității unei semnalări la nivel național, care poate fi adăugat semnalărilor în vederea arestării, semnalărilor privind persoane dispărute și semnalărilor în vederea efectuării de controale discrete, de verificări prin interviu și de controale specifice în cazul în care un stat membru consideră că faptul de a da curs unei semnalări este incompatibil cu dreptul său național, cu obligațiile sale internaționale sau cu interesele sale naționale fundamentale. În cazul în care semnalării i s-a aplicat un indicator de validitate, acțiunea care trebuie întreprinsă pe baza semnalării nu se întreprinde pe teritoriul respectivului stat membru;
- (i) „stat membru semnalant” înseamnă statul membru care a introdus semnalarea în SIS;
- (j) „stat membru executant” înseamnă statul membru care întreprinde sau a întreprins 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) „date dactiloscopice” înseamnă datele privind amprente digitale și amprente 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;

- (m) „infrațiune gravă” înseamnă infracțiunile menționate la articolul 2 alineatele (1) și (2) din Decizia-cadru 2002/584/JAI din 13 iunie 2002<sup>71</sup>;
- (n) „infracțiuni de terorism” înseamnă infracțiunile prevăzute de dreptul național menționate la articolele 1-4 din Decizia-cadru 2002/475/JAI din 13 iunie 2002<sup>72</sup>.

#### 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, „bază 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 dintre 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) în cazul obiectelor și datele enumerate la articolul 20 alineatul (3) literele (a)-(v) din prezentul regulament în cazul semnalărilor privind persoane. 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, Securitate și Justiție, instituită prin Regulamentul (UE) nr. 1077/2011<sup>73</sup> („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,

<sup>71</sup> 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).

<sup>72</sup> Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO L 164, 22.6.2002, p. 3).

<sup>73</sup> 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).

cu condiția ca fiecare dintre acestea să fie în măsură să prelucrez 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 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 53 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 61, 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 72 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 adoptă prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 72 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 66, 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 43.

#### *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, datele utilizate pentru efectuarea unei căutări, o referință cu privire la datele 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 articolele 40, 41 și 42, 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.
7. În cazul în care statele membre efectuează căutări automate prin scanarea plăcuțelor de înmatriculare a autovehiculelor, prin utilizarea sistemelor de recunoaștere automată a plăcuțelor de înmatriculare, acestea păstrează înregistrările căutărilor în conformitate cu dreptul național. Conținutul acestor înregistrări se stabilește prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2). În cazul în care se obține o corespondență în urma consultării datelor stocate în SIS sau într-o copie națională sau tehnică a SIS, se efectuează o căutare completă în SIS pentru a se verifica dacă respectiva corespondență este reală. Acestei căutări complete i se aplică dispozițiile prezentului articol alineatele (1)-(6).

*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 în mod periodic după acordarea accesului la datele din SIS, personalul autorităților care au un 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 prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 72 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 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 64, 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 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 40, 41 și 42, înregistrările arată, în special, tipul de date utilizate pentru efectuarea căutării, 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**

### **CATEGORII DE DATE ȘI APLICAREA UNUI INDICATOR DE VALIDITATE**

#### *Articolul 20* *Categoriile de date*

1. Fără a aduce atingere articolului 8 alineatul (1) sau dispozițiilor prezentului regulament care prevăd stocarea datelor suplimentare, SIS conține doar categoriile de date care sunt furnizate de fiecare stat membru și care sunt necesare pentru scopurile prevăzute la articolele 26, 32, 34, 36 și 38.
2. Categoriile de date sunt următoarele:
  - (a) informații privind persoanele care fac obiectul unei semnalări;
  - (b) informații privind obiectele menționate la articolele 32, 36 și 38.
3. 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 53;
  - (p) tipul de infracțiune pentru care s-a emis semnalarea;
  - (q) numărul de înregistrare al persoanei în cauză într-un registru național;
  - (r) o clasificare a tipului de caz de persoană dispărută (numai pentru semnalările menționate la articolul 32);
  - (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) profilurile ADN relevante, sub rezerva articolului 22 alineatul (1) litera (b) din prezentul regulament;
  - (y) date dactiloscopice;
  - (z) o copie color a documentului de identitate.
4. Normele tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatele (2) și (3) 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 72 alineatul (2).
5. Normele tehnice necesare pentru efectuarea de căutări în datele menționate la alineatul (3) se stabilesc și se precizează în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2). Aceste norme tehnice sunt similare în cazul căutărilor în CS-SIS, în copiile naționale și în copiile tehnice, astfel cum se menționează la articolul 53 alineatul (2), 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 72 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. În cazul în care un stat membru caută o persoană sau un obiect în legătură cu o infracțiune care intră sub incidența articolelor 1-4 din Decizia-cadru 2002/475/JAI a

Consiliului privind combaterea terorismului, acesta creează, în toate circumstanțele, semnalarea corespunzătoare prevăzută la articolul 34, 36 sau 38, după caz.

#### *Articolul 22*

##### *Norme specifice privind introducerea fotografiilor, a imaginilor faciale, a datelor dactiloscopice și a profilurilor ADN*

1. Introducerea în SIS a datelor menționate la articolul 20 alineatul (3) literele (w), (x) și (y) face obiectul următoarelor dispoziții:
  - (a) fotografiile, imaginile faciale, datele dactiloscopice și profilurile ADN se introduc doar în urma unei verificări a calității pentru a se asigura îndeplinirea unui standard minim de calitate a datelor;
  - (b) se poate adăuga un profil ADN doar la semnalările prevăzute la articolul 32 alineatul (2) literele (a) și (c) și numai în cazul în care nu sunt disponibile fotografii, imagini faciale sau date dactiloscopice care să permită identificarea. Profilurile ADN ale persoanelor care sunt ascendenți direcți, descendenți sau frați ori surori ale persoanei care face obiectul semnalării pot fi adăugate la semnalare cu condiția ca persoanele în cauză să își dea acordul explicit. Originea rasială a persoanei nu se include în profilul ADN.
2. Pentru stocarea datelor menționate la prezentul articol alineatul (1) litera (a) și la articolul 40 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 72 alineatul (2).

#### *Articolul 23*

##### *Cerințe privind introducerea unei semnalări*

1. O semnalare privind o persoană nu poate fi introdusă fără datele prevăzute la articolul 20 alineatul (3) literele (a), (g), (k), (m), (n) și, dacă este cazul, (p), cu excepția situațiilor menționate la articolul 40.
2. În cazul în care sunt disponibile, se introduc, de asemenea, toate celelalte date menționate la articolul 20 alineatul (3).

#### *Articolul 24*

##### *Dispoziții generale privind aplicarea unui indicator de validitate*

1. În cazul în care un stat membru consideră că faptul de a da curs unei semnalări introduse în conformitate cu articolele 26, 32 și 36 este incompatibil cu dreptul său național, cu obligațiile sale internaționale sau cu interesele sale naționale fundamentale, acesta poate solicita ulterior ca semnalării să i se aplice un indicator de validitate care să arate că acțiunea care trebuie întreprinsă pe baza semnalării nu va fi întreprinsă pe teritoriul său. Indicatorul de validitate se aplică de către biroul SIRENE al statului membru semnalant.
2. Pentru ca statele membre să poată solicita ca unei semnalări emise în conformitate cu articolul 26 să i se adauge un indicator de validitate, tuturor statelor membre li se notifică în mod automat orice nouă semnalare din categoria respectivă, prin intermediul schimbului de informații suplimentare.
3. Dacă în cazuri extrem de urgente și de grave un stat membru semnalant solicită executarea acțiunii, statul membru care execută semnalarea examinează dacă poate să autorizeze retragerea indicatorului de validitate aplicat la cererea sa. Dacă statul

membru executant este în măsură să facă acest lucru, ia măsurile necesare pentru se asigura că acțiunea care trebuie întreprinsă poate să fie efectuată imediat.

#### *Articolul 25*

##### *Aplicarea unui indicator de validitate semnalărilor în vederea arestării în scopul predării*

1. În cazul în care se aplică Decizia-cadru 2002/584/JAI, unei semnalări în vederea arestării în scopul predării i se adaugă un indicator de validitate care împiedică arestarea numai atunci când autoritatea judiciară competentă în temeiul dreptului național să execute un mandat european de arestare a refuzat executarea acestuia pe baza unui motiv de neexecutare și atunci când s-a solicitat aplicarea indicatorului de validitate.
2. Cu toate acestea, la cererea unei autorități judiciare competente în temeiul dreptului național, pe baza unei instrucțiuni generale sau într-un caz specific, se poate solicita, de asemenea, ca unei semnalări în vederea arestării în scopul predării să i se aplice un indicator de validitate dacă este evident că executarea mandatului european de arestare va trebui să fie refuzată.

## **CAPITOLUL VI**

### **SEMNALĂRILE PRIVIND PERSOANE CĂUTATE ÎN VEDEREA ARESTĂRII ÎN SCOPUL PREDĂRII SAU AL EXTRĂDĂRII**

#### *Articolul 26*

##### *Obiectivele semnalărilor și condițiile de emitere a acestora*

1. Datele privind persoane căutate în vederea arestării în scopul predării pe baza unui mandat european de arestare sau căutate în vederea arestării în scopul extradării se introduc la cererea autorității judiciare a statului membru semnalant.
2. Datele privind persoane căutate în vederea arestării în scopul predării se introduc, de asemenea, pe baza mandatelor de arestare emise în conformitate cu acordurile încheiate între Uniunea Europeană și țările terțe în temeiul articolului 37 din Tratatul privind Uniunea Europeană în scopul predării persoanelor pe baza unui mandat de arestare, care prevăd transmiterea acestui mandat de arestare prin intermediul SIS.
3. Orice trimitere din prezentul regulament la dispozițiile Deciziei-cadru 2002/584/JAI trebuie înțeleasă ca incluzând dispozițiile corespunzătoare ale acordurilor încheiate între Uniunea Europeană și țările terțe în temeiul articolului 37 din Tratatul privind Uniunea Europeană în scopul predării persoanelor pe baza unui mandat de arestare care prevăd transmiterea acestui mandat de arestare prin intermediul SIS.
4. În cazul unei operațiuni de căutare în curs și în urma autorizării de către autoritatea judiciară competentă din statul membru semnalant, acesta poate să suspende temporar disponibilitatea unei semnalări existente în vederea arestării emise în temeiul articolului 26 din prezentul regulament, astfel încât semnalarea să nu fie inclusă în rezultatul căutărilor efectuate de utilizatorul final și să fie accesibilă doar birourilor SIRENE. Această funcționalitate se utilizează pentru o perioadă de maximum 48 de ore. În cazul în care este necesar din punct de vedere operațional, această perioadă poate fi însă prelungită cu perioade suplimentare de 48 de ore. Statele membre întocmesc statistici referitoare la numărul de semnalări în cazul cărora s-a utilizat această funcționalitate.

#### *Articolul 27*

##### *Date suplimentare privind persoane căutate în vederea arestării în scopul predării*

1. În cazul în care o persoană este căutată în vederea arestării în scopul predării pe baza unui mandat european de arestare, statul membru semnalant introduce în SIS o copie a originalului mandatului european de arestare.
2. Statul membru semnalant poate introduce o copie a traducerii mandatului european de arestare în una sau mai multe limbi oficiale ale instituțiilor Uniunii Europene.

#### *Articolul 28*

##### *Informații suplimentare privind persoane căutate în vederea arestării în scopul predării*

Statul membru care a introdus în SIS semnalarea în vederea arestării în scopul predării comunică celorlalte state membre informațiile menționate la articolul 8 alineatul (1) din Decizia-cadru 2002/584/JAI, prin intermediul schimbului de informații suplimentare.

#### *Articolul 29*

##### *Informații suplimentare privind persoane căutate în vederea arestării în scopul extrădării*

1. Statul membru care a introdus în SIS semnalarea în vederea arestării în scopul extrădării comunică celorlalte state membre, prin intermediul schimbului de informații suplimentare, următoarele informații:
  - (a) autoritatea care a emis cererea de arestare;
  - (b) dacă există un mandat de arestare sau un document cu același efect juridic ori o hotărâre executorie;
  - (c) natura infracțiunii și încadrarea juridică a acesteia;
  - (d) o descriere a circumstanțelor în care s-a comis infracțiunea, inclusiv data, locul și măsura în care persoana care face obiectul semnalării a participat la comiterea infracțiunii;
  - (e) în măsura în care este posibil, consecințele infracțiunii;
  - (f) orice alte informații utile sau necesare pentru executarea semnalării.
2. Datele menționate la alineatul (1) nu se comunică în cazul în care datele menționate la articolul 27 sau 28 au fost deja furnizate și sunt considerate suficiente pentru executarea semnalării de către statul membru în cauză.

#### *Articolul 30*

##### *Conversia semnalărilor privind persoane căutate în vederea arestării în scopul predării sau al extrădării*

În cazul în care nu se poate efectua arestarea, fie din cauza refuzului unui stat membru solicitat, exprimat în conformitate cu procedurile privind aplicarea unui indicator de validitate stabilite la articolul 24 sau 25, fie, în cazul unei semnalări în vederea arestării în scopul extrădării, pentru că investigația nu s-a finalizat, statul membru solicitat tratează semnalarea ca o semnalare în scopul comunicării locului unde se află persoana vizată.

### Articolul 31

#### *Executarea acțiunii solicitate într-o semnalare privind o persoană căutată în vederea arestării în scopul predării sau al extrădării*

1. O semnalare introdusă în SIS în conformitate cu articolul 26, împreună cu datele suplimentare menționate la articolul 27, constituie și are același efect ca un mandat european de arestare emis în conformitate cu Decizia-cadru 2002/584/JAI, în cazul în care se aplică decizia-cadru menționată.
2. În cazul în care nu se aplică Decizia-cadru 2002/584/JAI, o semnalare introdusă în SIS în conformitate cu articolele 26 și 29 produce aceleași efecte juridice ca o cerere de arestare provizorie în temeiul articolului 16 din Convenția europeană de extrădare din 13 decembrie 1957 sau al articolului 15 din Tratatul Benelux privind extrădarea și asistența reciprocă judiciară în materie penală din 27 iunie 1962.

## CAPITOLUL VII

### SEMNALĂRILE PRIVIND PERSOANE DISPĂRUTE

#### Articolul 32

##### *Obiectivele semnalărilor și condițiile de emitere a acestora*

1. Datele privind persoane dispărute sau alte persoane care trebuie plasate sub protecție ori despre care nu se știe unde se află se introduc în SIS la cererea autorității competente din statul membru care a emis semnalarea.
2. Se pot introduce următoarele categorii de persoane dispărute:
  - (a) persoane dispărute care trebuie plasate sub protecție
    - (i) pentru propria lor protecție;
    - (i) pentru a preveni amenințări;
  - (b) persoane dispărute care nu trebuie plasate sub protecție;
  - (c) copii expuși riscului de răpire în conformitate cu alineatul (4).
3. Alineatul (2) litera (a) se aplică în special copiilor și persoanelor care trebuie să facă obiectul internării în urma unei decizii emise de o autoritate competentă.
4. O semnalare privind un copil din categoria menționată la alineatul 2 litera (c) se introduce la cererea autorității judiciare competente din statul membru care este competent în materia răspunderii părintești în conformitate cu Regulamentul nr. 2201/2003 al Consiliului <sup>74</sup> în cazul în care există un risc concret și evident ca respectivul copil să fie scos în mod ilegal și iminent din statul membru în care este situată autoritatea judiciară competentă. În statele membre care sunt părți contractante la Convenția de la Haga din 19 octombrie 1996 asupra competenței, legii aplicabile, recunoașterii, executării și cooperării privind răspunderea părintească și măsurile de protecție a copiilor și în cazul în care nu se aplică Regulamentul nr. 2201/2003 al Consiliului, sunt aplicabile dispozițiile Convenției de la Haga.

<sup>74</sup>

Regulamentul (CE) nr. 2201/2003 al Consiliului din 27 noiembrie 2003 privind competența, recunoașterea și executarea hotărârilor judecătorești în materie matrimonială și în materia răspunderii părintești, de abrogare a Regulamentului (CE) nr. 1347/2000 (JO L 338, 23.12.2003, p. 1).

5. Statele membre se asigură că datele introduse în SIS indică în care dintre categoriile menționate la alineatul (2) se încadrează persoana dispărută. În plus, statele membre se asigură, de asemenea, că datele introduse în SIS indică despre ce tip de caz de persoană dispărută sau vulnerabilă este vorba. Normele detaliate privind clasificarea tipurilor de cazuri și introducerea acestor date se stabilesc și se precizează prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).
6. Cu patru luni înainte ca un copil care face obiectul unei semnalări prevăzute la prezentul articol să împlinească vârsta majoratului, CS-SIS notifică în mod automat statului membru semnalant că este necesar ca motivul cererii și acțiunea care trebuie întreprinsă să fie actualizate sau ca semnalarea să fie ștearsă.
7. În cazul în care există indicii clare că anumite vehicule, ambarcațiuni sau aeronave au legătură cu o persoană care face obiectul unei semnalări prevăzute la alineatul (2), se pot emite semnalări privind vehiculele, ambarcațiunile și aeronavele respective pentru a localiza persoana vizată. În aceste cazuri se creează o conexiune între semnalarea privind persoana dispărută și semnalarea privind obiectul, în conformitate cu articolul 60. Normele tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la prezentul alineat 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 72 alineatul (2).

### *Articolul 33*

#### *Executarea acțiunii solicitate într-o semnalare*

1. În cazul în care o persoană menționată la articolul 32 este localizată, autoritățile competente comunică, sub rezerva alineatului (2), statului membru care a emis semnalarea unde se află aceasta. În cazul copiilor dispăruți sau al copiilor care trebuie plasați sub protecție, statul membru executant consultă imediat statul membru semnalant pentru a se ajunge fără întârziere la un acord privind măsurile care trebuie luate pentru a proteja interesul superior al copilului. În cazurile menționate la articolul 32 alineatul (2) literele (a) și (c), autoritățile competente pot să transfere persoana respectivă într-un loc sigur pentru a o împiedica să își continue călătoria, dacă dreptul național permite acest lucru.
2. Comunicarea datelor, alta decât cea dintre autoritățile competente, privind o persoană dispărută care a fost localizată și care este majoră se face numai cu acordul respectivei persoane. Cu toate acestea, autoritățile competente pot comunica persoanei care a raportat dispariția faptul că semnalarea a fost ștearsă, deoarece persoana dispărută a fost localizată.

## **CAPITOLUL VIII**

### **SEMNALĂRILE PRIVIND PERSOANE CĂUTATE ÎN VEDEREA PARTICIPĂRII LA O PROCEDURĂ JUDICIARĂ**

#### *Articolul 34*

##### *Obiectivele semnalărilor și condițiile de emitere a acestora*

1. Pentru a comunica locul de reședință sau domiciliul persoanelor, statele membre introduc în SIS, la cererea unei autorități competente, date privind:

- (a) martori;
  - (b) persoane citate sau căutate pentru a fi citate să se prezinte în fața autorităților judiciare în cadrul unei proceduri penale pentru a răspunde în legătură cu fapte de care sunt acuzate;
  - (c) persoane cărora trebuie să li se notifice sau comunice o hotărâre judecătorească sau alte documente privind o procedură penală pentru a răspunde în legătură cu fapte de care sunt acuzate;
  - (d) persoane cărora trebuie să li se notifice sau comunice o citație pentru a se prezenta în vederea executării unei pedepse privative de libertate.
2. În cazul în care există indicii clare că anumite vehicule, ambarcațiuni sau aeronave au legătură cu o persoană care face obiectul unei semnalări prevăzute la alineatul (1), se pot emite semnalări privind vehiculele, ambarcațiunile și aeronavele respective pentru a localiza persoana vizată. În aceste cazuri se creează o conexiune între semnalările privind persoana și semnalarea privind obiectul, în conformitate cu articolul 60. Normele tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la prezentul alineat 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 72 alineatul (2).

#### *Articolul 35*

#### *Executarea acțiunii solicitate într-o semnalare*

Informațiile cerute i se comunică statului membru solicitant prin intermediul schimbului de informații suplimentare.

## **CAPITOLUL IX**

### **SEMNALĂRILE PRIVIND PERSOANE ȘI OBIECTE ÎN SCOPUL EFECTUĂRII DE CONTROALE DISCRETE, DE VERIFICĂRI PRIN INTERVIU SAU DE CONTROALE SPECIFICE**

#### *Articolul 36*

#### *Obiectivele semnalărilor și condițiile de emitere a acestora*

1. Datele privind persoane sau vehicule, ambarcațiuni, aeronave și containere se introduc în conformitate cu dreptul național al statului membru care emite semnalarea, în scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice, astfel cum se prevede la articolul 37 alineatul (4).
2. Semnalarea poate fi emisă în scopul urmăririi penale a infracțiunilor, al executării unei pedepse penale și al prevenirii amenințărilor la adresa siguranței publice:
  - (a) în cazul în care există indicii clare că o persoană intenționează să comită sau comite o infracțiune gravă, în special infracțiunile menționate la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI;
  - (b) în cazul în care informațiile menționate la articolul 37 alineatul (1) sunt necesare pentru executarea unei pedepse penale a unei persoane condamnate pentru o infracțiune gravă, în special infracțiunile menționate la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI sau

- (c) în cazul în care în urma evaluării generale a unei persoane, în special pe baza infracțiunilor pe care aceasta le-a comis în trecut, există motive să se creadă că respectiva persoană va comite și în viitor infracțiuni grave, în special infracțiunile menționate la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI.
3. În plus, se poate emite o semnalare în conformitate cu dreptul național, la cererea autorităților responsabile cu securitatea națională, dacă există indicii concrete că informațiile menționate la articolul 37 alineatul (1) sunt necesare pentru a preveni o amenințare gravă din partea persoanei vizate sau alte amenințări grave la adresa securității naționale interne sau externe. Statul membru care emite semnalarea prevăzută la prezentul alineat informează celelalte state membre cu privire la aceasta. Fiecare stat membru stabilește autoritățile cărora li se transmite această informație.
4. În cazul în care există indicii clare că anumite vehicule, ambarcațiuni, aeronave și containere au legătură cu infracțiunile grave menționate la alineatul (2) sau cu amenințările grave menționate la alineatul (3), se pot emite semnalări privind vehiculele, ambarcațiunile, aeronavele și containerele respective.
5. În cazul în care există indicii clare că documente oficiale în alb sau documente de identitate eliberate au legătură cu infracțiunile grave menționate la alineatul (2) sau cu amenințările grave menționate la alineatul (3), se pot emite semnalări privind documentele respective, indiferent de identitatea eventualului titular inițial al documentului de identitate. Normele tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la prezentul alineat 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 72 alineatul (2).

### *Articolul 37*

#### *Executarea acțiunii solicitate într-o semnalare*

1. În scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice, toate sau unele dintre următoarele informații se colectează și se comunică autorității care a emis semnalarea atunci când pe teritoriul unui stat membru se efectuează controale sau verificări la frontiere, verificări polițienești și vamale sau alte activități de asigurare a respectării legii:
- (a) faptul că s-a localizat persoana sau vehiculul, ambarcațiunea, aeronava, containerul, documentul oficial în alb sau documentul de identitate eliberat care face obiectul unei semnalări;
  - (b) locul, ora și motivul efectuării verificării;
  - (c) ruta și destinația călătoriei;
  - (d) persoanele care însoțesc persoana vizată sau ocupanții vehiculului, ai ambarcațiunii ori ai aeronavei sau persoanele care îl însoțesc pe titularul documentului oficial în alb sau al documentului de identitate eliberat despre care se poate presupune în mod rezonabil că au legătură cu persoanele vizate;
  - (e) identitatea dezvăluită și descrierea persoanei care utilizează documentul oficial în alb sau documentul de identitate eliberat care face obiectul semnalării;
  - (f) vehiculul, ambarcațiunea, aeronava sau containerul utilizat;
  - (g) obiectele transportate, inclusiv documentele de călătorie;

- (h) circumstanțele în care s-a localizat persoana sau vehiculul, ambarcațiunea, aeronava, containerul, documentul oficial în alb sau documentul de identitate eliberat.
- 2. Informațiile menționate la alineatul (1) se comunică prin intermediul schimbului de informații suplimentare.
- 3. În funcție de circumstanțele operaționale și în conformitate cu dreptul național, un control discret cuprinde o verificare de rutină a unei persoane sau a unui obiect cu scopul de a colecta cât mai multe dintre informațiile menționate la alineatul (1), pe cât posibil fără a pune în pericol caracterul discret al controlului.
- 4. În funcție de circumstanțele operaționale și în conformitate cu dreptul național, o verificare prin interviu cuprinde o verificare mai aprofundată și interogarea persoanei. În cazul în care dreptul unui stat membru nu autorizează verificările prin interviu, acestea se înlocuiesc în respectivul stat membru cu controale discrete.
- 5. În timpul controalelor specifice, vehiculele, ambarcațiunile, aeronavele, containerele și obiectele transportate pot fi percheziționate în conformitate cu dreptul național în scopurile menționate la articolul 36. Perchezițiile se efectuează în conformitate cu dreptul național. În cazul în care dreptul unui stat membru nu autorizează controalele specifice, acestea se înlocuiesc în respectivul stat membru cu verificări prin interviu.

## **CAPITOLUL X**

### **SEMNALĂRILE PRIVIND OBIECTE CĂUTATE PENTRU A FI CONFISCATE SAU FOLOSITE CA PROBE ÎN CADRUL PROCEDURILOR PENALE**

#### *Articolul 38*

#### *Obiectivele semnalărilor și condițiile de emitere a acestora*

- 1. Datele privind obiecte căutate pentru a fi confiscate sau folosite ca probe în cadrul procedurilor penale se introduc în SIS.
- 2. Se introduc următoarele categorii de obiecte ușor identificabile:
  - (a) vehicule cu motor, astfel cum sunt definite de dreptul național, indiferent de sistemul de propulsie;
  - (b) remorci cu o greutate fără încărcătură de peste 750 kg;
  - (c) rulote;
  - (d) echipamente industriale;
  - (e) ambarcațiuni;
  - (f) motoare de ambarcațiuni;
  - (g) containere;
  - (h) aeronave;
  - (i) arme de foc;
  - (j) documente oficiale în alb care au fost furate, însușite în mod ilegal sau pierdute;

- (k) documente de identitate eliberate, cum ar fi pașapoarte, cărți de identitate, permise de conducere, permise de ședere și documente de călătorie care au fost furate, însușite în mod ilegal, pierdute sau anulate ori care se pretind a fi astfel de documente, dar sunt falsificate;
  - (l) certificate sau plăcuțe de înmatriculare a vehiculelor care au fost furate, însușite în mod ilegal, pierdute sau invalidate ori care se pretind a fi astfel de documente ori plăcuțe, dar sunt falsificate;
  - (m) bancnote (bancnote înregistrate) și bancnote falsificate;
  - (n) echipamente tehnice, produse din domeniul tehnologiei informației și alte obiecte ușor identificabile de mare valoare;
  - (o) componente identificabile ale autovehiculelor;
  - (p) componente identificabile ale echipamentelor industriale.
3. Definiția noilor subcategorii de obiecte de la alineatul (2) litera (n) și 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 72 alineatul (2).

#### *Articolul 39*

##### *Executarea acțiunii solicitate într-o semnalare*

1. În cazul în care în urma unei căutări în date se identifică o semnalare privind un obiect care a fost localizat, autoritatea care a stabilit corespondența celor două elemente de date confiscă, în conformitate cu dreptul național, obiectul și contactează autoritatea care a emis semnalarea pentru a se ajunge la un acord privind măsurile care trebuie luate. În acest scop, se pot comunica și date cu caracter personal, în conformitate cu prezentul regulament.
2. Informațiile menționate la alineatul (1) se comunică prin intermediul schimbului de informații suplimentare.
3. Statul membru care a localizat obiectul ia măsurile solicitate în conformitate cu dreptul național.

## **CAPITOLUL XI**

### **SEMNALĂRILE PRIVIND PERSOANE CĂUTATE NECUNOSCUTE ÎN SCOPUL IDENTIFICĂRII ÎN CONFORMITATE CU DREPTUL NAȚIONAL ȘI EFECTUAREA DE CĂUTĂRI CU AJUTORUL DATELOR BIOMETRICE**

#### *Articolul 40*

##### *Semnalările privind persoane căutate necunoscute în scopul reținerii în temeiul dreptului național*

În SIS se pot introduce date dactiloscopice care nu au legătură cu persoane care fac obiectul semnalărilor. Aceste date dactiloscopice sunt seturi complete sau incomplete de amprente digitale sau de amprente palmare descoperite la locul unor infracțiuni în curs de investigare, al unei infracțiuni grave și al unei infracțiuni de terorism și despre care se poate stabili cu un grad ridicat de probabilitate că aparțin autorului infracțiunii. Datele dactiloscopice din această

categorie se stochează cu mențiunea „persoană căutată sau suspectată necunoscută”, cu condiția ca autoritățile competente să nu poată stabili identitatea respectivei persoane prin utilizarea niciunei alte baze de date naționale, europene sau internaționale.

#### *Articolul 41*

##### *Executarea acțiunii solicitate într-o semnalare*

În cazul obținerii unui rezultat pozitiv sau a unei potențiale corespondențe cu datele stocate prevăzute la articolul 40, identitatea persoanei se stabilește în conformitate cu dreptul național și se verifică dacă datele dactiloscopice stocate în SIS aparțin respectivei persoane. Statele membre comunică prin intermediul schimbului de informații suplimentare pentru a facilita investigarea în timp util a cazului.

#### *Articolul 42*

##### *Norme specifice privind verificarea fotografiilor, a imaginilor faciale, a datelor dactiloscopice și a profilurilor ADN sau efectuarea de căutări cu ajutorul acestora*

1. Fotografiile, imaginile faciale, datele dactiloscopice și profilurile ADN 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. În datele dactiloscopice stocate în SIS se efectuează căutări 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 26, al articolului 34 alineatul (1) literele (b) și (d) și al articolului 36 se pot efectua, de asemenea, căutări utilizând 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 la punctele obișnuite de trecere a frontierei în cazul în care se utilizează sisteme de control self-service și sisteme de control automat la frontieră.

## **CAPITOLUL XII**

### **DREPTUL DE ACCES LA SEMNALĂRI ȘI PĂSTRAREA ACESTORA**

#### *Articolul 43*

##### *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:
  - (a) controlul la frontieră, 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.
2. 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 procedurilor penale și cu anchetele judiciare anterioare punerii sub acuzare, în îndeplinirea sarcinilor care le revin, astfel cum se prevede în dreptul național, precum și de către autoritățile lor coordonatoare.
3. Dreptul de acces la datele introduse în SIS și de a efectua căutări în aceste date în mod direct poate fi exercitat de autoritățile competente pentru efectuarea sarcinilor prevăzute la alineatul (1) litera (c) în îndeplinirea sarcinilor respective. Accesul acestor autorități este reglementat de dreptul fiecărui stat membru.
4. Autoritățile menționate la prezentul articol sunt incluse pe lista prevăzută la articolul 53 alineatul (8).

#### *Articolul 44*

##### *Autoritățile de înmatriculare a vehiculelor*

1. Serviciile din statele membre responsabile cu eliberarea certificatelor de înmatriculare a vehiculelor, astfel cum se menționează în Directiva 1999/37/CE a Consiliului<sup>75</sup>, au acces la următoarele date introduse în SIS în conformitate cu articolul 38 alineatul (2) literele (a), (b), (c) și (l) din prezentul regulament doar în scopul de a verifica dacă vehiculele care le sunt prezentate pentru înmatriculare au fost furate, însușite în mod ilegal sau pierdute ori dacă sunt căutate pentru a fi folosite ca probe în cadrul unor proceduri penale:
- (a) date privind autovehiculele, astfel cum sunt definite de dreptul național, indiferent de sistemul de propulsie;
  - (b) date privind remorcile cu o greutate fără încărcătură de peste 750 kg și rulotele;
  - (c) date privind certificatele de înmatriculare și plăcuțele de înmatriculare ale vehiculelor care au fost furate, însușite în mod ilegal sau anulate.
- Accesul la aceste date al serviciilor responsabile cu eliberarea certificatelor de înmatriculare pentru vehicule este reglementat de dreptul național al respectivului stat membru.
2. Serviciile menționate la alineatul (1) care sunt servicii publice au dreptul de a accesa în mod direct datele introduse în SIS.
3. Serviciile menționate la alineatul (1) care nu sunt servicii publice au dreptul de a accesa datele introduse în SIS numai prin intermediul unei autorități menționate la

<sup>75</sup>

Directiva 1999/37/CE a Consiliului din 29 aprilie 1999 privind documentele de înmatriculare pentru vehicule (JO L 138, 1.6.1999, p. 57).

articolul 43 din prezentul regulament. Această autoritate are dreptul de a accesa în mod direct respectivele date și de a le transmite serviciului în cauză. Statul membru în cauză se asigură că serviciul respectiv și personalul acestuia au obligația de a respecta eventualele limitări impuse în ceea ce privește condițiile de utilizare a datelor care le sunt transmise de către autoritate.

4. Articolul 39 din prezentul regulament nu se aplică accesului obținut în conformitate cu prezentul articol. Comunicarea de către serviciile menționate la alineatul (1) poliției sau autorităților judiciare a oricărei informații care a fost obținută datorită accesului la SIS și care generează suspiciunea comiterii unei infracțiuni este reglementată de dreptul național.

#### *Articolul 45*

##### *Autoritățile de înmatriculare a ambarcațiunilor și a aeronavelor*

1. Serviciile din statele membre responsabile cu eliberarea certificatelor de înmatriculare sau cu asigurarea gestionării traficului pentru ambarcațiuni, inclusiv motoare de ambarcațiuni, și aeronave au acces la următoarele date introduse în SIS în conformitate cu articolul 38 alineatul (2) din prezentul regulament doar în scopul de a verifica dacă ambarcațiunile, inclusiv motoarele de ambarcațiuni, aeronavele sau containerele care le sunt prezentate pentru înmatriculare sau care fac obiectul gestionării traficului au fost furate, însușite în mod ilegal sau pierdute ori dacă sunt căutate pentru a fi folosite ca probe în cadrul unor proceduri penale:
  - (a) date privind ambarcațiuni;
  - (b) date privind motoare de ambarcațiuni;
  - (c) date privind aeronave.

Sub rezerva alineatului (2), dreptul fiecărui stat membru reglementează accesul acestor servicii la datele respective în statul membru în cauză. Accesul la datele enumerate la literele (a)-(c) de mai sus se limitează la competența specifică a serviciilor în cauză.

2. Serviciile menționate la alineatul (1) care sunt servicii publice au dreptul de a accesa în mod direct datele introduse în SIS.
3. Serviciile menționate la alineatul (1) care nu sunt servicii publice au dreptul de a accesa datele introduse în SIS numai prin intermediul unei autorități menționate la articolul 43 din prezentul regulament. Această autoritate are dreptul de a accesa în mod direct datele și de a le transmite serviciului în cauză. Statul membru în cauză se asigură că serviciul respectiv și personalul acestuia au obligația de a respecta eventualele limitări impuse în ceea ce privește condițiile de utilizare a datelor care le sunt transmise de către autoritatea respectivă.
4. Articolul 39 din prezentul regulament nu se aplică accesului obținut în conformitate cu prezentul articol. Comunicarea de către serviciile menționate la alineatul (1) poliției sau autorităților judiciare a oricărei informații care a fost obținută datorită accesului la SIS și care generează suspiciunea comiterii unei infracțiuni este reglementată de dreptul național.

*Articolul 46*  
*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 după caz.
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 47

##### *Accesul Eurojust la datele din SIS*

1. Membrii naționali ai Eurojust și asistenții acestora au dreptul, în limitele mandatului lor, de a accesa și de a efectua căutări în datele introduse în SIS, în conformitate cu articolele 26, 32, 34, 38 și 40.
2. În cazul în care o căutare efectuată de un membru național al Eurojust indică existența unei semnalări în SIS, acesta informează statul membru semnalant.
3. Nicio dispoziție a prezentului articol nu trebuie interpretată ca aducând atingere dispozițiilor Deciziei 2002/187/JAI referitoare la protecția datelor și la răspunderea pentru orice prelucrare neautorizată sau incorectă a acestor date de către membrii naționali ai Eurojust sau asistenții acestora ori ca afectând competențele Organismului comun de supraveghere instituit în temeiul deciziei menționate.
4. Fiecare accesare și fiecare căutare efectuate de un membru național al Eurojust sau de un asistent al acestuia se înregistrează în conformitate cu dispozițiile articolului 12 și fiecare utilizare de către aceștia a datelor accesate se înregistrează.
5. Nicio parte a SIS nu se conectează la un sistem informatic pentru colectarea și prelucrarea datelor efectuate de Eurojust sau în cadrul acestuia și nici nu se transferă către un astfel de sistem datele din SIS la care au acces membrii naționali sau asistenții acestora. Nicio parte a SIS nu se descarcă. Înregistrarea accesului și a căutărilor nu se consideră a constitui o descărcare sau o copiere ilegală a datelor din SIS.
6. Accesul la datele introduse în SIS se limitează la membrii naționali și la asistenții acestora și nu se extinde la personalul Eurojust.
7. Se adoptă și se aplică măsuri pentru asigurarea securității și a confidențialității, astfel cum se prevede la articolele 10 și 11.

#### Articolul 48

##### *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 49 alineatul (1).
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 49*

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

1. În sensul articolului 48 alineatul (1) și al alineatului (2) al prezentului articol, Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă înființează și întreține o interfață tehnică care permite conectarea directă la SIS central.
2. 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 26, 32, 34 și 36 și cu articolul 38 alineatul (2) literele (j) și (k), în scopul de a-și îndeplini sarcinile care i-au fost atribuite prin Regulamentul de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS).
3. În cazul în care o verificare efectuată de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă 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).
4. 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.
5. 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 aceasta a datelor pe care le-a accesat se înregistrează.
6. 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.

7. Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă adoptă și aplică măsuri de asigurare a securității și a confidențialității, astfel cum se prevede la articolele 10 și 11.

#### *Articolul 50*

##### *Domeniul de aplicare al accesului*

Utilizatorii finali, inclusiv Europol, membrii naționali ai Eurojust și asistenții acestora, precum 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 51*

##### *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. Semnalările emise în scopurile articolului 36 din prezentul regulament se păstrează pentru o perioadă maximă de un an.
3. Semnalările privind documente oficiale în alb și documente de identitate eliberate introduse în conformitate cu articolul 38 se păstrează maximum 10 ani. Pentru categoriile de semnalări privind obiecte se pot stabili perioade de păstrare mai scurte prin intermediul unor măsuri de punere în aplicare adoptate în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).
4. Fiecare stat membru stabilește, după caz, perioade de reexaminare mai scurte, în conformitate cu dreptul său național.
5. 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.
6. 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.
7. 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 (6). CS-SIS informează în mod automat statele

membre cu privire la ștergerea programată a datelor din sistem, cu patru luni în avans.

8. Statele membre întocmesc statistici privind numărul semnalărilor a căror perioadă de păstrare a fost prelungită în conformitate cu alineatul (6).

## **CAPITOLUL XIII**

### **ȘTERGEREA SEMNALĂRILOR**

#### *Articolul 52*

#### *Ștergerea semnalărilor*

1. Semnalările în vederea arestării în scopul predării sau al extrădării prevăzute la articolul 26 trebuie șterse după ce persoana în cauză a fost predată sau extrădată autorităților competente din statul membru semnalant. Ștergerea se poate efectua, de asemenea, atunci când hotărârea judecătorească în temeiul căreia s-a emis semnalarea a fost revocată de către autoritatea judiciară competentă conform dreptului național.
2. Semnalările privind persoane dispărute trebuie șterse în conformitate cu următoarele norme:
  - (a) în ceea ce privește copiii dispăruți, astfel cum se prevede la articolul 32, o semnalare trebuie ștearsă:
    - după soluționarea cazului, de exemplu, atunci când copilul a fost repatriat sau autoritățile competente din statul membru executant au adoptat o decizie privind îngrijirea copilului;
    - la încetarea valabilității semnalării în conformitate cu articolul 51;
    - după adoptarea unei decizii de către autoritatea competentă a statului membru semnalant sau
    - după localizarea copilului;
  - (b) în ceea ce privește adulții dispăruți, astfel cum se prevede la articolul 32, în cazul în care nu se solicită măsuri de protecție, o semnalare trebuie ștearsă:
    - după executarea acțiunii care trebuie întreprinsă (statul membru executant a stabilit locul unde se află persoana);
    - la încetarea valabilității semnalării în conformitate cu articolul 51 sau
    - după adoptarea unei decizii de către autoritatea competentă a statului membru semnalant;
  - (c) în ceea ce privește adulții dispăruți, astfel cum se prevede la articolul 32, în cazul în care se solicită măsuri de protecție, o semnalare trebuie ștearsă:
    - după executarea acțiunii care trebuie întreprinsă (persoana a fost plasată sub protecție);
    - la încetarea valabilității semnalării în conformitate cu articolul 51 sau

- după adoptarea unei decizii de către autoritatea competentă a statului membru semnalant.

Sub rezerva dreptului național, în cazul în care o persoană a fost internată în urma deciziei unei autorități competente, o semnalare poate fi păstrată până la repatrierea respectivei persoane.

3. Semnalările privind persoane căutate în vederea participării la o procedură judiciară trebuie șterse în conformitate cu următoarele norme:

În ceea ce privește semnalările privind persoane căutate în vederea participării la o procedură judiciară prevăzute la articolul 34, o semnalare trebuie ștersă:

- (a) după ce locul unde se află persoana a fost comunicat autorității competente a statului membru semnalant. În cazul în care nu se pot întreprinde acțiuni pe baza informațiilor transmise, biroul SIRENE al statului membru semnalant informează biroul SIRENE al statului membru executant pentru a soluționa problema;
- (b) la încetarea valabilității semnalării în conformitate cu articolul 51 sau
- (c) după adoptarea unei decizii de către autoritatea competentă a statului membru semnalant.

În cazul în care s-a obținut un rezultat pozitiv într-un stat membru, iar datele privind adresa au fost transmise statului membru semnalant și un rezultat pozitiv obținut ulterior în respectivul stat membru indică aceleași date privind adresa, rezultatul pozitiv se înregistrează în statul membru executant, însă nu se retrimite statului membru semnalant nici datele privind adresa, nici informații suplimentare. În aceste cazuri, statul membru executant informează statul membru semnalant cu privire la rezultatele pozitive repetate și statul membru semnalant analizează necesitatea de a menține semnalarea.

4. Semnalările în scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice trebuie șterse în conformitate cu următoarele norme:

În ceea ce privește semnalările în scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice prevăzute la articolul 36, o semnalare trebuie ștersă:

- (a) la încetarea valabilității semnalării în conformitate cu articolul 51;
- (b) după adoptarea de către autoritatea competentă a statului membru semnalant a unei decizii de ștergere a acesteia.

5. Semnalările privind obiecte căutate pentru a fi confiscate sau folosite ca probe trebuie șterse în conformitate cu următoarele norme:

În ceea ce privește ștergerea semnalărilor privind obiecte căutate pentru a fi confiscate sau folosite ca probe în cadrul unor proceduri penale prevăzute la articolul 38, o semnalare trebuie ștersă:

- (a) după confiscarea obiectului sau în cazul unei măsuri echivalente după efectuarea schimbului necesar ulterior de informații suplimentare între birourile SIRENE sau atunci când obiectul este vizat de o altă procedură judiciară sau administrativă;
- (b) la încetarea valabilității semnalării sau
- (c) după adoptarea de către autoritatea competentă a statului membru semnalant a unei decizii de ștergere a acesteia.

6. Semnalările privind persoane căutate necunoscute prevăzute la articolul 40 trebuie șterse în conformitate cu următoarele norme:
7. (a) după identificarea persoanei sau
8. (b) la încetarea valabilității semnalării.

## **CAPITOLUL XIV**

### **NORME GENERALE DE PRELUCRARE A DATELOR**

#### *Articolul 53*

#### *Prelucrarea datelor din SIS*

1. Statele membre pot prelucra datele menționate la articolul 20 numai în scopurile prevăzute pentru fiecare categorie de semnalări menționată la articolele 26, 32, 34, 36, 38 și 40.
2. Datele se pot copia doar în scopuri tehnice, cu condiția ca această copiere să fie necesară pentru ca autoritățile menționate la articolul 43 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.
4. 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.
5. Accesul la date este autorizat numai în limitele competenței autorităților naționale menționate la articolul 43 și numai pentru personalul autorizat în mod corespunzător.
6. În ceea ce privește semnalările prevăzute la articolele 26, 32, 34, 36, 38 și 40 din prezentul regulament, orice prelucrare a informațiilor conținute de acestea în alte scopuri decât cele pentru care au fost introduse în SIS trebuie să 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.
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 54*  
*Datele din SIS și fișierele naționale*

1. Articolul 53 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 53 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 55*  
*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 56*  
*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 59.
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 57*  
*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 naționale de supraveghere. 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 58*

##### *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 56 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 59*

##### *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) fotografii și 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 72 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 60* *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 menționată la articolul 72 alineatul (2).

#### *Articolul 61*

##### *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 62*

##### *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.

#### *Articolul 63*

##### *Schimbul de date cu Interpol privind pașapoarte furate, însușite ilegal, pierdute sau anulate*

1. Prin derogare de la articolul 62, se poate face schimb de informații introduse în SIS cu membrii Interpol în ceea ce privește numărul pașaportului, țara care l-a eliberat și tipul de pașaport furat, însușit în mod ilegal, pierdut sau anulat, prin stabilirea unei conexiuni între SIS și baza de date a Interpol privind documente de călătorie furate sau pierdute, sub rezerva încheierii unui acord între Interpol și Uniunea Europeană. Acordul trebuie să prevadă că transmiterea datelor introduse de un stat membru este condiționată de acordul respectivului stat membru.
2. Acordul menționat la alineatul (1) trebuie să prevadă că datele transmise sunt accesibile doar membrilor Interpol din țări care asigură un nivel de protecție adecvat al datelor cu caracter personal. Înainte de încheierea acestui acord, Consiliul solicită avizul Comisiei referitor la adecvarea nivelului de protecție al datelor cu caracter personal și respectarea drepturilor și libertăților fundamentale în ceea ce privește prelucrarea automată a datelor cu caracter personal de către Interpol și țările care au membri delegați la Interpol.
3. Acordul menționat la alineatul (1) poate prevedea, de asemenea, accesul statelor membre prin intermediul SIS la datele din baza de date a Interpol privind documente

de călătorie furate sau pierdute, în conformitate cu dispozițiile relevante ale prezentei decizii care reglementează semnalările introduse în SIS privind pașapoarte furate, însușite în mod ilegal, pierdute și anulate.

## CAPITOLUL XV

### PROTECȚIA DATELOR

#### *Articolul 64*

##### *Legislația aplicabilă*

1. Regulamentul (CE) nr. 45/2001 se aplică prelucrării datelor cu caracter personal de către agenție în temeiul prezentului regulament.
2. Regulamentul (UE) 2016/679 se aplică prelucrării datelor cu caracter personal 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 65*

##### *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. Orice persoană are dreptul ca datele care o privesc care conțin erori de fapt sau care au fost stocate ilegal să fie șterse.
  6. 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.
  7. 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 66*

##### *Căi de atac*

1. Orice persoană poate introduce o acțiune în fața instanțelor judecătorești sau a autorității competente în temeiul dreptului oricărui stat membru pentru accesarea, rectificarea sau ștergerea informațiilor ori pentru obținerea de informații sau 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 70.
3. Pentru a se obține o imagine de ansamblu coerentă asupra funcționării căilor de atac, autoritățile naționale elaborează 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 69.

*Articolul 67*  
*Supravegherea N.SIS*

1. Fiecare stat membru se asigură că autoritatea (autoritățile) națională(e) de supraveghere desemnată(e) în fiecare stat membru și investită(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 lor 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 68*  
*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 69*  
*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 XVI**

### **RĂSPUNDEREA**

#### *Articolul 70 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 XVII**

### **DISPOZIȚII FINALE**

#### *Articolul 71 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. Statisticile întocmite nu conțin date cu caracter personal. Raportul statistic anual se publică. Agenția furnizează, de asemenea, statistici anuale privind utilizarea funcționalității de suspendare temporară, în cazul efectuării de căutări, a disponibilității unei semnalări emise în temeiul articolului 26 din prezentul regulament, în total și pentru fiecare stat membru, inclusiv orice prelungire a perioadei de indisponibilitate de 48 de ore.
4. Statele membre, precum și Europol, Eurojust și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă furnizează agenției și Comisiei informațiile necesare pentru elaborarea rapoartelor menționate la alineatele (3), (7) și (8). Aceste informații includ statistici separate privind numărul de căutări efectuate de serviciile din statele membre responsabile cu eliberarea certificatelor de înmatriculare a vehiculelor și de serviciile din statele membre responsabile cu eliberarea certificatelor de înmatriculare sau cu asigurarea gestionării traficului pentru ambarcațiuni, inclusiv motoare de ambarcațiuni, aeronave și containere, sau în numele respectivelor servicii. Statisticile menționează, de asemenea, numărul de rezultate pozitive pentru fiecare categorie de semnalări.
5. Agenția furnizează statelor membre, Comisiei, Europol, Eurojust 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), (4) și (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 prezentul 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, Eurojust 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 normele privind protecția datelor și securitatea aplicabile registrului se adoptă prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 72 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 72* *Procedura comitetului*

1. Comisia este asistată de 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 73* *Modificări aduse Regulamentului (UE) nr. 515/2014*

Regulamentul (UE) nr. 515/2014<sup>76</sup> 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.....).”*

#### *Articolul 74* *Abrogare*

La data aplicării prezentului regulament se abrogă următoarele acte juridice:

Regulamentul (CE) nr. 1986/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind accesul la Sistemul de Informații Schengen din a doua generație (SIS II) al serviciilor competente, în statele membre, pentru eliberarea certificatelor de înmatriculare a vehiculelor;

Decizia 533/2007/JAI a Consiliului din 12 iulie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II);

---

<sup>76</sup> 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).

Decizia 2010/261/UE a Comisiei din 4 mai 2010 privind planul de securitate pentru SIS II central și infrastructura de comunicații<sup>77</sup>;

*Articolul 75*

*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,  
Președintele*

*Pentru Consiliu,  
Președintele*

---

<sup>77</sup>

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).

## **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 cooperării polițienești și al cooperării judiciare în materie penală, de modificare a Regulamentului (UE) nr. 515/2014 și de abrogare a Regulamentului (CE) nr. 1986/2006, a Deciziei 2007/533/JAI a Consiliului și a Deciziei 2010/261/UE a Comisiei.

#### 1.2. Domeniul (domeniile) de politică în cauză în structura ABM/ABB<sup>78</sup>

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**<sup>79</sup>
- ☒ 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 – „Demantelarea criminalității organizate”

Obiectiv – „Un răspuns ferm al UE în materie de combatere a terorismului și de prevenire a radicalizării”

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 securitatea”<sup>80</sup>, Comisia și-a anunțat intenția de a evalua SIS în perioada 2015-2016 și de a analiza dacă există noi nevoi operaționale care impun modificări legislative. De asemenea, în Agenda privind securitatea s-a subliniat faptul că SIS ocupă un loc central în ceea ce privește schimburile de informații în domeniul polițienesc și ar trebui să fie consolidat în continuare. Mai recent, în Comunicarea sa intitulată „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”<sup>81</sup>, Comisia a declarat că va analiza, pe baza raportului privind evaluarea globală, introducerea unor funcționalități suplimentare ale sistemului și prezentarea de propuneri de revizuire a temeiului juridic al SIS. În fine, la 20 aprilie 2016, în Comunicarea sa intitulată „Punerea în aplicare a Agendei europene privind securitatea pentru a combate terorismul și a deschide calea către o uniune a securității efectivă și autentică”<sup>82</sup>,

<sup>78</sup> ABM (activity based management): gestiune pe activități – ABB (activity based budgeting): întocmirea bugetului pe activități.

<sup>79</sup> Astfel cum sunt menționate la articolul 54 alineatul (2) litera (a) sau (b) din Regulamentul financiar.

<sup>80</sup> COM(2015) 185 final.

<sup>81</sup> COM(2016) 205 final.

<sup>82</sup> COM(2016) 230 final.

Comisia a propus o serie de modificări ale SIS menite să îmbunătățească valoarea sa adăugată în scopul asigurării respectării legii.

Evaluarea globală, efectuată de Comisie, a confirmat faptul că SIS este un succes operațional. Totuși, în pofida numeroaselor realizări ale sistemului, în urma evaluării s-au formulat, de asemenea, o serie de recomandări care vizează îmbunătățirea eficacității și a eficienței tehnice și operaționale ale acestuia.

Pe baza recomandărilor din raportul privind evaluarea globală și în deplină concordanță cu obiectivele Comisiei prezentate în comunicările menționate mai sus și în Planul strategic pentru perioada 2016-2020 al DG Migrație și Afaceri Interne<sup>83</sup>, prezenta propunere vizează să pună în aplicare:

- anunțul Comisiei privind îmbunătățirea valorii adăugate a SIS în scopul asigurării respectării legii pentru a răspunde noilor amenințări;
- recomandările privind modificările tehnice și procedurale care rezultă dintr-o evaluare cuprinzătoare a SIS;
- solicitările privind îmbunătățiri tehnice primite din partea utilizatorilor finali;
- constatările provizorii ale Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate în ceea ce privește calitatea datelor.

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 2.1 – Un răspuns ferm al UE în materie de combatere a terorismului și de prevenire a radicalizării;

Obiectivul specific 2.2. – Demantelarea criminalității transfrontaliere grave și organizate.

Activitatea (activitățile) ABM/ABB în cauză

Capitolul 18 02 – Securitate internă

### 1.4.3. *Rezultatul (rezultatele) și impactul preconizate*

*A se preciza efectele pe care propunerea/inițiativa ar trebui să le aibă asupra beneficiarilor vizați/grupurilor vizate.*

Scopul principal al modificărilor juridice și tehnice ale SIS prevăzute în propunere este de a spori eficacitatea acestuia din punct de vedere operațional. 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 cooperării în materie de asigurare a respectării legii.

Noua propunere introduce măsuri care abordează nevoile tehnice și operaționale ale utilizatorilor finali. În special, noile câmpuri de date pentru semnalările existente vor permite agenților de poliție 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 activitatea agenților de asigurare a respectării legii. De asemenea, prezenta propunere prevede modificări tehnice care vor face ca sistemul să devină mai eficient și care îl vor simplifica.

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.

Propunerea introduce noi elemente biometrice de identificare – amprente palmare, imagini faciale și profiluri ADN – în cazuri specifice și limitate. Noutatea menționată, împreună cu modificările propuse ale articolelor 32 și 33 (semnalările privind persoane dispărute) pentru a permite introducerea de semnalări preventive și împărțirea pe categorii a cazurilor de persoane dispărute, în primul rând va întări în mod semnificativ protecția minorilor neînsoțiți și, în al doilea rând, va permite identificarea lor pe baza profilului lor ADN sau al celui al părinților sau al celui al fraților ori surorilor (cu acordul acestora).

Autoritățile statelor membre vor putea, de asemenea, să emită semnalări privind persoane necunoscute căutate în legătură cu o infracțiune doar pe baza amprentelor digitale sau a amprentelor palmare latente sau prelevate de la locul infracțiunii. Acest lucru nu este posibil în temeiul actualului cadru juridic și tehnic și, prin urmare, constituie o evoluție importantă.

### 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 propunerii 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 adăugarea unor noi elemente la categoriile de semnalări existente 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 Sistemului de informații Schengen 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 obținute 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. În plus, agenția va furniza, de asemenea, statistici anuale privind utilizarea funcționalității de suspendare temporară, în cazul efectuării de căutări, a disponibilității unei semnalări emise în temeiul articolului 26 din prezentul regulament, în total și pentru fiecare stat membru, inclusiv orice prelungire a perioadei de indisponibilitate de 48 de ore.

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 va trimite evaluarea Parlamentului European și Consiliului.

Obiectivul specific 1 – „Demantelarea criminalității organizate”.

Indicator – Utilizarea mecanismelor UE în materie de schimb de informații. Realizarea acestui obiectiv poate fi măsurată prin creșterea numărului de rezultate pozitive obținute în SIS. Indicatorii sunt rapoartele statistice întocmite de eu-LISA și de statele membre, care vor permite Comisiei să evalueze cum sunt utilizate noile funcționalități ale sistemului.

Obiectivul specific 2 – Un răspuns ferm al UE în materie de combatere a terorismului și de prevenire a radicalizării.

Indicator – Sporirea numărului de semnalări și de rezultate pozitive, în special în legătură cu articolul 36 alineatul (3) din propunere, care vizează semnalările privind persoane și obiecte în scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice.

## **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. O mai bună armonizare a procedurilor naționale de utilizare a SIS.
3. Extinderea listei de utilizatori instituționali care au acces la datele din SIS, prin acordarea unui acces deplin la sistem Europol și noii Agenții Europene pentru Poliția de Frontieră și Garda de Coastă.
4. Adăugarea de noi elemente semnalărilor din SIS și de noi funcționalități pentru a extinde domeniul de aplicare al sistemului, pentru a-i permite acestuia să facă față mediului de securitate actual, pentru a întări cooperarea dintre autoritățile statelor membre de asigurare a respectării legii și din domeniul securității și pentru a reduce sarcina administrativă.
5. Abordarea utilizării complete a SIS de la un capăt la altul, care include nu numai sistemul central și sistemele naționale, ci și asigură faptul că utilizatorii finali primesc toate datele necesare pentru a-și îndeplini sarcinile.
6. Întărirea asigurării continuității activității și garantarea funcționării neîntrerupte a SIS la nivel central și național.
7. Consolidarea luptei împotriva criminalității internaționale, a terorismului și a criminalității informatice, care constituie domenii interdependente, cu o puternică dimensiune transfrontalieră.

#### 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. Obiectivele propunerii 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, face 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 competente ale statelor membre au accesat sistemul de aproape 2,9 miliarde de ori, ceea ce demonstrează în mod clar contribuția esențială a sistemului la cooperarea în materie de asigurare a respectării legii în spațiul Schengen. Acest nivel ridicat al schimbului de informații dintre statele membre nu ar fi fost atins prin intermediul unor soluții naționale 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 statele membre ale UE. În plus, Europol și noua Agenție 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. *Învățămintele desprinse din experiențe anterioare similare*

1. Faza de dezvoltare ar trebui să înceapă numai după definirea integrală a nevoilor operaționale și a cerințelor utilizatorilor finali. 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 cu părțile interesate relevante, inclusiv cu 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 într-un mod foarte transparent și cuprinzător în cadrul unor reuniuni și ateliere specifice. 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 două studii, ale căror constatări au fost utilizate la elaborarea prezentei propuneri:

- Evaluarea tehnică a SIS (*SIS Technical Assessment*) – 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*) – 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.

### 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”<sup>84</sup>, 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.

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

a) securitatea internă, astfel cum s-a subliniat în Agenda europeană privind securitatea<sup>85</sup>, pentru a preveni, a depista, a investiga și a urmări penal infracțiunile grave și infracțiunile de terorism, permițând autorităților de asigurare a respectării

<sup>84</sup> COM(2016) 205 final.

<sup>85</sup> COM(2015) 185 final.

legii să prelucrez datele cu caracter personal ale persoanelor suspectate de a fi implicate în acte de terorism sau în infracțiuni grave;

b) protecția datelor, în măsura în care prezenta propunere trebuie să asigure 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) Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă<sup>86</sup> în ceea ce privește, în primul rând, posibilitatea ca personalul agenției să efectueze analize ale riscurilor și, în al doilea rând, accesul acestuia la SIS în scopurile sistemului ETIAS propus. Propunerea vizează, de asemenea, să furnizeze o interfață tehnică pentru accesul la 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 pentru ca, în limitele mandatului lor, acestea să aibă dreptul de a accesa și de a efectua căutări în datele introduse în SIS;

b) Europol, în măsura în care propunerea îi acordă acestuia drepturi suplimentare de acces la datele introduse în SIS și de efectuare de căutări în aceste date, în limitele mandatului său;

c) Prüm, în măsura în care dezvoltările prevăzute în prezenta propunere menite să permită identificarea persoanelor pe baza amprentelor digitale (precum și pe baza imaginilor faciale și a profilurilor ADN) completează dispozițiile Prüm existente<sup>87</sup> privind accesul online transfrontalier reciproc la bazele de date ADN și sistemele automate de identificare a amprentelor digitale naționale desemnate.

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

a) gestionarea frontierelor externe. Propunerea completează noul principiu preconizat în Codul frontierelor Schengen, astfel cum a fost instituit ca răspuns la fenomenul luptătorilor teroriști străini, privind efectuarea de verificări sistematice, în bazele de date relevante, ale tuturor călătorilor, inclusiv ale cetățenilor UE, la intrarea și la ieșirea din spațiul Schengen;

b) sistemul de intrare/ieșire<sup>88</sup> (EES), în măsura în care prezenta propunere urmărește să reflecte utilizarea unei combinații de amprente digitale și imagini faciale ca elemente biometrice de identificare pentru funcționarea EES;

<sup>86</sup> 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).

<sup>87</sup> Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008, p. 1) și Decizia 2008/616/JAI a Consiliului din 23 iunie 2008 privind punerea în aplicare a Deciziei 2008/615/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008, p. 12).

<sup>88</sup> 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 privește pe resortisanții țărilor terțe care trec frontierele externe

c) ETIAS, în măsura în care prezenta propunere ține seama de acest sistem propus care prevede o evaluare aprofundată în materie de securitate, inclusiv o verificare în SIS, a resortisanților țărilor terțe care intenționează să călătorească în Uniunea Europeană.

### 1.6. Durata și impactul financiar

- ☐ Propunere/inițiativă pe **durată determinată**
  - ☐ Propunere/inițiativă în vigoare din [ZZ/LL]AAAA până la [ZZ/LL]AAAA
  - ☐ Impact financiar din AAAA până în AAAA
- ☒ Propunere/inițiativă pe **durată nedeterminată**
  - perioada pregătitoare: 2017
  - 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)<sup>89</sup>

- ☒ **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 dintre propuneri [prezenta propunere și Propunerea de regulament privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere] 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.**

<sup>89</sup>

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

## **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 71 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.

În plus, eu-LISA este de acum însărcinată și cu furnizarea de statistici zilnice, lunare și anuale privind utilizarea SIS și cu asigurarea monitorizării continue a sistemului și a funcționării sale în raport cu obiectivele.

### **2.2. 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, eu-LISA 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 eu-LISA.

#### 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 fraudă, 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 Informatică 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. <sup>90</sup> | Țări AELS <sup>91</sup> | Țări candidate <sup>92</sup> | 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                                                                           |

<sup>90</sup> Dif. = credite diferențiate / Nedif. = credite nediferențiate.

<sup>91</sup> AELS: Asociația Europeană a Liberului Schimb.

<sup>92</sup> 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

|                                                 |   |                         |
|-------------------------------------------------|---|-------------------------|
| <b>Rubrica din cadrul financiar multianual:</b> | 3 | Securitate și cetățenie |
|-------------------------------------------------|---|-------------------------|

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

|                                                 |          |                                |
|-------------------------------------------------|----------|--------------------------------|
| <b>Rubrica din cadrul financiar multianual:</b> | <b>3</b> | <b>Securitate și cetățenie</b> |
|-------------------------------------------------|----------|--------------------------------|

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

### 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)   |  |  |  |  |  |  |  |  |
| <b>TOTAL credite</b>                                                              | Angajamente | =4+ 6 |  |  |  |  |  |  |  |  |

|                                                                           |       |       |  |  |  |  |  |  |  |  |
|---------------------------------------------------------------------------|-------|-------|--|--|--|--|--|--|--|--|
| <b>în cadrul RUBRICII &lt;....&gt;</b><br>din cadrul financiar multianual | 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)   |        |        |        |  |  |  |               |
| <b>TOTAL credite</b><br><b>în cadrul RUBRICILOR 1-4</b><br>din cadrul financiar multianual<br>(Suma de referință) | Angajamente | =4+ 6 | 19,337 | 22,520 | 22,451 |  |  |  | <b>64,308</b> |
|                                                                                                                   | Plăți       | =5+ 6 | 8,944  | 28,362 | 25,120 |  |  |  | <b>62,426</b> |

**3.2.3. Impactul estimat asupra creditelor cu caracter administrativ**

|                                                 |          |                             |
|-------------------------------------------------|----------|-----------------------------|
| <b>Rubrica din cadrul financiar multianual:</b> | <b>5</b> | „Cheltuieli administrative” |
|-------------------------------------------------|----------|-----------------------------|

|                                  |         | Anul<br>N | Anul<br>N+1 | Anul<br>N+2 | Anul<br>N+3 | A se introduce atâtia ani câți<br>sunt considerați necesari pentru<br>a reflecta durata impactului<br>(cf. punctul 1.6) |  |  | TOTAL |
|----------------------------------|---------|-----------|-------------|-------------|-------------|-------------------------------------------------------------------------------------------------------------------------|--|--|-------|
| DG: <.....>                      |         |           |             |             |             |                                                                                                                         |  |  |       |
| • Resursele umane                |         |           |             |             |             |                                                                                                                         |  |  |       |
| • Alte cheltuieli administrative |         |           |             |             |             |                                                                                                                         |  |  |       |
| <b>TOTAL DG &lt;.....&gt;</b>    | Credite |           |             |             |             |                                                                                                                         |  |  |       |

milioane EUR (cu trei zecimale)

|                                                                              |                                      |  |  |  |  |  |  |  |  |
|------------------------------------------------------------------------------|--------------------------------------|--|--|--|--|--|--|--|--|
| <b>TOTAL credite<br/>pentru RUBRICA 5</b><br>din cadrul financiar multianual | (Total angajamente =<br>Total plăți) |  |  |  |  |  |  |  |  |
|------------------------------------------------------------------------------|--------------------------------------|--|--|--|--|--|--|--|--|

milioane EUR (cu trei zecimale)

|                                                                                      |             | Anul<br>N <sup>93</sup> | Anul<br>N+1 | Anul<br>N+2 | Anul<br>N+3 | A se introduce atâtia ani câți<br>sunt considerați necesari pentru<br>a reflecta durata impactului<br>(cf. punctul 1.6) |  |  | TOTAL |
|--------------------------------------------------------------------------------------|-------------|-------------------------|-------------|-------------|-------------|-------------------------------------------------------------------------------------------------------------------------|--|--|-------|
| <b>TOTAL credite<br/>în cadrul RUBRICILOR 1-5</b><br>din cadrul financiar multianual | Angajamente |                         |             |             |             |                                                                                                                         |  |  |       |
|                                                                                      | Plăți       |                         |             |             |             |                                                                                                                         |  |  |       |

<sup>93</sup>

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

### 3.2.3.1 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<br>obiectivele și<br>realizările                               |           |                   | Anul<br>2018         |     | Anul<br>2019 |        | Anul<br>2020 |        | A se introduce atâția ani câți sunt considerați<br>necesari pentru a reflecta durata impactului<br>(cf. punctul 1.6) |     |             |     |             |     | TOTAL       |     |             |              |
|----------------------------------------------------------------------------|-----------|-------------------|----------------------|-----|--------------|--------|--------------|--------|----------------------------------------------------------------------------------------------------------------------|-----|-------------|-----|-------------|-----|-------------|-----|-------------|--------------|
|                                                                            | REALIZĂRI |                   |                      |     |              |        |              |        |                                                                                                                      |     |             |     |             |     |             |     |             |              |
|                                                                            | ↓         | Tip <sup>94</sup> | Costur<br>i<br>medii | Nr. | Costur<br>i  | Nr.    | Costur<br>i  | Nr.    | Costur<br>i                                                                                                          | Nr. | Costur<br>i | Nr. | Costu<br>ri | Nr. | Costur<br>i | Nr. | Costur<br>i | Nr.<br>total |
| OBIECTIVUL SPECIFIC NR. 1 <sup>95</sup><br>Dezvoltarea sistemului național |           |                   | 1                    |     | 1            | 1,221  | 1            | 1,221  |                                                                                                                      |     |             |     |             |     |             |     |             | 2,442        |
| OBIECTIVUL SPECIFIC NR. 2<br>Infrastructură                                |           |                   | 1                    |     | 1            | 17,184 | 1            | 17,184 |                                                                                                                      |     |             |     |             |     |             |     |             | 34,368       |
| COSTURI TOTALE                                                             |           |                   |                      |     |              | 18,405 |              | 18,405 |                                                                                                                      |     |             |     |             |     |             |     |             | 36,810       |

<sup>94</sup> 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.).

<sup>95</sup> Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)...”

### 3.2.3.2 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:

Credite de angajament în milioane EUR (cu trei zecimale)

| A se indica obiectivele și realizările<br><br>↓                           |                   |                | 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 <sup>96</sup> | Costur i medii | Nr.       | Costur i | Nr.       | Costur i | Nr.       | Costur i | Nr.                                                                                                            | Costur i | Nr. | Costu ri | Nr. | Costur i | Nr.   | Costur i | Nr. total | Costuri totale |
| OBIECTIVUL SPECIFIC NR. 1 <sup>97</sup><br>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<br>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          |

<sup>96</sup> 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.).  
<sup>97</sup> Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)...”

|                                               |   |        |   |       |   |       |  |  |  |  |  |  |  |  |  |        |
|-----------------------------------------------|---|--------|---|-------|---|-------|--|--|--|--|--|--|--|--|--|--------|
| Subtotal pentru obiectivul specific nr. 2     |   |        |   | 1,913 |   | 1,913 |  |  |  |  |  |  |  |  |  | 3,826  |
| OBIECTIVUL SPECIFIC NR. 3<br>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  |
| <b>COSTURI TOTALE</b>                         |   | 12,893 |   | 2,051 |   | 1,982 |  |  |  |  |  |  |  |  |  | 16,926 |

### 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<br>2018 | Anul<br>2019 | Anul<br>2020 | TOTAL |
|--|--------------|--------------|--------------|-------|
|--|--------------|--------------|--------------|-------|

|                            |       |       |       |       |
|----------------------------|-------|-------|-------|-------|
| Funcționari (grade AD)     |       |       |       |       |
| Funcționari (grade AST)    |       |       |       |       |
| Agenți contractuali        | 0,210 | 0,210 | 0,210 | 0,630 |
| Agenți temporari           |       |       |       |       |
| Experți naționali detașați |       |       |       |       |

|              |              |              |              |              |
|--------------|--------------|--------------|--------------|--------------|
| <b>TOTAL</b> | <b>0,210</b> | <b>0,210</b> | <b>0,210</b> | <b>0,630</b> |
|--------------|--------------|--------------|--------------|--------------|

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 durată 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<br>1<br>N | Anul<br>1<br>N+1 | Anul N+2 | An<br>ul<br>N+<br>3 | A se<br>introdu<br>ce<br>atâtia<br>ani câți<br>sunt<br>conside<br>rați<br>necesari<br>pentru<br>a<br>reflecta<br>durata<br>impact<br>ului<br>(cf. pu<br>nctul<br>1.6) |  |  |
|---------------------------------------------------------------------------|----------------|------------------|----------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
| <b>• Posturi din schema de personal (funcționari și agenți temporari)</b> |                |                  |          |                     |                                                                                                                                                                       |  |  |
| 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)                                           |                |                  |          |                     |                                                                                                                                                                       |  |  |
| <b>• Personal extern (în echivalent normă întreagă: ENI)<sup>98</sup></b> |                |                  |          |                     |                                                                                                                                                                       |  |  |
| 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 <sup>99</sup>                                                 | - 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)                                        |                |                  |          |                     |                                                                                                                                                                       |  |  |
| <b>TOTAL</b>                                                              |                |                  |          |                     |                                                                                                                                                                       |  |  |

**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:

<sup>98</sup> 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.

<sup>99</sup> 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 referitoare la actualizarea funcționalităților SIS II, 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<br>N | Anul<br>N+1 | Anul<br>N+2 | Anul<br>N+3 | A se introduce atâția ani câți sunt<br>considerați necesari pentru a<br>reflecta durata impactului<br>(cf. punctul 1.6) |  |  | Total |
|------------------------------------------------------|-----------|-------------|-------------|-------------|-------------------------------------------------------------------------------------------------------------------------|--|--|-------|
| A se preciza organismul<br>care asigură cofinanțarea |           |             |             |             |                                                                                                                         |  |  |       |
| TOTAL credite<br>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 <sup>100</sup> |      |      |      |                                                                                                                |  |  |
|--------------------------------------------------------------------------------------|---------------------------------------------------------|------------------------------------------------|------|------|------|----------------------------------------------------------------------------------------------------------------|--|--|
|                                                                                      |                                                         | 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.

<sup>100</sup>

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.