Regulament 1862 din 07-12-2018

Publicat în Jurnalul Oficial L nr. 312 din 07-12-2018

REGULAMENTUL (UE) 2018/1862 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 28 noiembrie 2018

privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală, de modificare și de abrogare a Deciziei 2007/533/JAI a Consiliului și de abrogare a Regulamentului (CE) nr. 1986/2006 al Parlamentului European și al Consiliului și a Deciziei 2010/261/UE a Comisiei

Intrare în vigoare: 27/12/2018

Punere în aplicare: a se vedea art. 79

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 ([1]),

întrucât:

(1) Sistemul de informații Schengen (SIS) este un instrument esențial pentru aplicarea dispozițiilor acquis-ului Schengen, astfel cum este integrat în cadrul Uniunii Europene. SIS este una dintre cele mai importante măsuri compensatorii care contribuie la menținerea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție al Uniunii, prin sprijinirea cooperării operaționale dintre autoritățile naționale competente, în special polițiștii de frontieră, poliție, autoritățile vamale, autoritățile din domeniul imigrației, autoritățile responsabile cu prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau cu executarea pedepselor.

(2) SIS a fost înființat inițial 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 ([2]) (denumită în continuare „Convenția de punere în aplicare a Acordului Schengen"). Dezvoltarea SIS de a doua generație (SIS II) a fost încredințată Comisiei în temeiul Regulamentului (CE) nr. 2424/2001 al Consiliului ([3]) și al Deciziei 2001/886/JAI a Consiliului ([4]). Acest sistem a fost instituit ulterior prin Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului ([5]) și prin Decizia 2007/533/JAI a Consiliului ([6]). SIS II a înlocuit SIS, astfel cum a fost creat în temeiul Convenției de punere în aplicare a Acordului Schengen.

(3) La trei ani de la intrarea în funcțiune a SIS II, Comisia a efectuat o evaluare a sistemului în conformitate cu Regulamentul (CE) nr. 1987/2006 și cu Decizia 2007/533/JAI. La 21 decembrie 2016, Comisia a prezentat Parlamentului European și Consiliului Raportul 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. Recomandările formulate în aceste documente ar trebui să se reflecte, după caz, în prezentul regulament.

(4) Prezentul regulament constituie temeiul juridic pentru SIS în ceea ce privește aspectele care intră în domeniul de aplicare al părții a treia titlul V capitolele 4 și 5 din Tratatul privind funcționarea Uniunii Europene (TFUE). Regulamentul (UE) 2018/1861 al Parlamentului European și al Consiliului ([7]) constituie temeiul juridic pentru SIS în ceea ce privește aspectele care intră în domeniul de aplicare al părții a treia titlul V capitolul 2 din TFUE.

(5) Faptul că temeiul juridic pentru SIS constă în instrumente separate nu afectează principiul conform căruia SIS constituie un sistem de informații unic, care ar trebui să funcționeze ca atare. Acesta ar trebui să cuprindă o rețea unică de birouri naționale denumite birourile SIRENE pentru a asigura schimbul de informații suplimentare. Prin urmare, anumite dispoziții ale instrumentelor respective ar trebui să fie identice.

(6) Este necesar să se specifice obiectivele SIS, anumite elemente ale arhitecturii sale tehnice și ale finanțării sale, să se stabilească norme privind funcționarea și utilizarea sa de la un capăt la altul, precum și să se definească responsabilitățile. Este necesar, de

asemenea, să se determine categoriile de date care urmează să fie introduse în sistem, scopurile introducerii și prelucrării acestora și criteriile introducerii acestora. De asemenea, sunt necesare norme care să reglementeze ștergerea semnalărilor, autoritățile abilitate să aibă acces la date, utilizarea datelor biometrice, și care să stabilească normele privind protecția datelor și prelucrarea datelor.

(7) Semnalările din SIS conțin doar informațiile necesare pentru identificarea unei persoane sau a unui obiect și pentru acțiunea de urmat. Prin urmare, statele membre ar trebui să facă schimb de informații suplimentare referitoare la semnalări atunci când acest lucru este necesar.

(8) SIS cuprinde un sistem central (SIS central) și sisteme naționale. Sistemele naționale ar putea să conțină o copie integrală sau parțială a bazei de date din SIS, care poate fi utilizată în comun de două sau mai multe state membre. Având în vedere că SIS este cel mai important instrument de schimb de informații în Europa pentru asigurarea securității și a gestionării eficace a frontierelor, este necesar să se asigure funcționarea sa neîntreruptă atât la nivel central, cât și la nivel național. Disponibilitatea SIS ar trebui să fie supusă unei monitorizări atente la nivel central și la nivelul statelor membre, iar orice incident de întrerupere a disponibilității pentru utilizatorii finali ar trebui înregistrat și raportat părților interesate de la nivel național și de la nivelul Uniunii. Fiecare stat membru ar trebui să creeze un sistem de rezervă pentru sistemul său național. De asemenea, statele membre ar trebui să asigure conectarea neîntreruptă cu SIS central prin intermediul unor puncte de conectare duplicate și separate din punct de vedere fizic și geografic. SIS central și infrastructura de comunicații ar trebui să fie operate astfel încât să se asigure funcționarea lor 24 de ore pe zi, șapte zile pe săptămână. Din acest motiv, Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție („eu-LISA”) instituită prin Regulamentul (UE) 2018/1726 al Parlamentului European și al Consiliului ([8]) ar trebui să pună în aplicare soluții tehnice care să facă mai sigură disponibilitatea neîntreruptă a SIS, care să fie supuse unei evaluări a impactului independente și unei analize cost-beneficiu.

(9) Este necesar să se întrețină un manual care să stabilească normele detaliate privind schimbul de informații suplimentare referitoare la acțiunile necesare ca urmare a semnalărilor (denumit în continuare „manualul SIRENE”). Birourile SIRENE ar trebui să asigure schimbul acestor informații în mod rapid și eficient.

(10) Pentru a se asigura schimbul eficient de informații suplimentare, inclusiv cu privire la acțiunea de urmat specificată în semnalări, este oportun să se consolideze funcționarea birourilor SIRENE prin precizarea cerințelor referitoare la resursele disponibile și la formarea utilizatorilor, precum și la timpul de răspuns la solicitările pe care le primesc din partea altor birouri SIRENE.

(11) Statele membre ar trebui să se asigure că personalul propriului birou SIRENE are competențele lingvistice și cunoștințele privind dreptul și normele procedurale relevante necesare pentru a-și îndeplini sarcinile.

(12) Pentru a fi în măsură să beneficieze pe deplin de funcționalitățile SIS, statele membre ar trebui să se asigure că utilizatorii finali și personalul birourilor SIRENE beneficiază periodic de formare, inclusiv cu privire la securitatea datelor, protecția datelor și calitatea datelor. Birourile SIRENE ar trebui să fie implicate în elaborarea programelor de formare. Pe cât posibil, birourile SIRENE ar trebui, de asemenea, să prevadă organizarea de schimburi de personal cu celelalte birouri SIRENE cel puțin o dată pe an. Statele membre sunt încurajate să ia măsurile necesare pentru ca schimbările de personal să nu conducă la pierderi de competențe și de experiență.

(13) Gestionarea operațională a componentelor centrale ale SIS este efectuată de eu-LISA. Pentru a permite eu-LISA să aloce resursele financiare și de personal necesare care să acopere toate aspectele legate de gestionarea operațională a SIS central și a infrastructurii de comunicații, prezentul regulament ar trebui să îi stabilească în detaliu sarcinile, în special în ceea ce privește aspectele tehnice ale schimbului de informații suplimentare.

(14) Fără a aduce atingere responsabilității statelor membre pentru exactitatea datelor introduse în SIS și nici rolului birourilor SIRENE de coordonatori de calitate, eu-LISA ar trebui să fie responsabilă cu îmbunătățirea calității datelor prin introducerea unui instrument central de monitorizare a calității datelor și ar trebui să furnizeze rapoarte Comisiei și statelor membre, la intervale regulate. Comisia ar trebui să prezinte Parlamentului European și Consiliului rapoarte referitoare la problemele întâmpinate cu privire la calitatea datelor. Pentru a îmbunătăți și mai mult calitatea datelor din SIS, eu-LISA ar trebui, de asemenea, să ofere formare privind utilizarea SIS organismelor de formare naționale și, pe cât posibil, birourilor SIRENE și utilizatorilor finali.

(15) Pentru a permite o mai bună monitorizare a utilizării SIS și a analiza tendințele în materie de infracțiuni, eu-LISA ar trebui să fie în măsură să dezvolte un sistem de ultimă generație în vederea elaborării de rapoarte statistice destinate statelor membre, Parlamentului European, Consiliului, Comisiei, Europol, Eurojust 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 central. Statisticile păstrate sau obținute din registrul respectiv nu ar trebui să conțină nici un fel de date cu caracter personal. Statele membre ar trebui să comunice statistici referitoare la exercitarea dreptului de acces, la rectificarea datelor inexacte și la ștergerea datelor stocate în mod ilegal, în cadrul cooperării dintre autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor în temeiul prezentului regulament.

(16) În SIS ar trebui introduse noi categorii 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 și a depista identitățile multiple, semnalarea ar trebui să includă în cazul în care astfel de informații sunt disponibile, o trimitere la documentul personal de identificare al persoanei în cauză sau la numărul acestuia și o copie a documentului, color dacă este posibil.

(17) Autoritățile competente ar trebui să fie în măsură, atunci când este strict necesar, să introducă în SIS informații specifice referitoare la orice caracteristici fizice specifice, obiective și inalterabile ale unei persoane, cum ar fi tatuajele, semnele sau

cicatricile.

(18) În cazul în care sunt disponibile, ar trebui introduse toate datele relevante, în special prenumele persoanei în cauză, atunci când se creează o semnalare, pentru a se reduce la minimum riscul de rezultate fals pozitive și activitățile operaționale inutile.

(19) SIS nu ar trebui să stocheze datele utilizate pentru efectuarea de căutări, cu excepția păstrării înregistrărilor cu scopul de a verifica dacă respectiva căutare este legală, pentru a monitoriza legalitatea prelucrării datelor, pentru automonitorizare și pentru a asigura funcționarea corespunzătoare a sistemelor naționale, precum și pentru integritatea și securitatea datelor.

(20) SIS ar trebui să permită prelucrarea datelor biometrice pentru a facilita identificarea fiabilă a persoanelor în cauză. Orice introducere în SIS a fotografiilor, a imaginilor faciale sau a datelor dactiloscopice și orice utilizare a unor astfel de date ar trebui să se limiteze la ceea ce este necesar pentru îndeplinirea obiectivelor urmărite, ar trebui să fie autorizată prin dreptul Uniunii, ar trebui să respecte drepturile fundamentale, inclusiv interesul superior al copilului, și ar trebui să fie în conformitate cu dreptul Uniunii în materie de protecție a datelor, inclusiv cu dispozițiile relevante privind protecția datelor prevăzute în prezentul regulament. În aceeași perspectivă, pentru a se evita inconvenientele cauzate de identificarea eronată a acestora, SIS ar trebui, de asemenea, să permită prelucrarea datelor privind persoanele a căror identitate a fost uzurpată, sub rezerva unor garanții adecvate, a obținerii acordului persoanei în cauză pentru fiecare categorie de date, în special pentru amprentele palmare și al unei limitări stricte a scopurilor în care aceste date cu caracter personal pot fi prelucrate în mod legal.

(21) 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, căutări în SIS în paralel, sub rezerva principiilor stabilite la articolul 4 din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului ([9]) și la articolul 5 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([10]). Astfel ar trebui să se garanteze că SIS funcționează ca principală măsură compensatorie în spațiul fără controale la frontierele interne și abordează mai bine dimensiunea transfrontalieră a criminalității și mobilitatea infractorilor.

(22) Prezentul regulament ar trebui să stabilească condițiile de utilizare a datelor dactiloscopice, a fotografiilor și a imaginilor faciale în scopul identificării și al verificării. În scopul identificării, imaginile faciale și fotografiile ar trebui folosite inițial numai în contextul punctelor obișnuite de trecere a frontierei. O astfel de folosire ar trebui să facă obiectul unui raport din partea Comisiei care să confirme dacă tehnologia este disponibilă, fiabilă și gata pentru a fi utilizată.

(23) Introducerea unui sistem automat de identificare a amprentelor digitale în cadrul SIS completează mecanismul Prüm existent privind accesul online transfrontalier reciproc la bazele naționale de date ADN și la sistemele naționale automate de identificare a amprentelor digitale desemnate, astfel cum se prevede în Deciziile 2008/615/JAI ([11]) și 2008/616/JAI ([12]) ale Consiliului. Căutarea în SIS a datelor dactiloscopice permite o căutare activă a autorului infracțiunii. Prin urmare, ar trebui să fie posibil să se încarce în SIS datele dactiloscopice ale unui autor necunoscut al unei infracțiuni, cu condiția ca persoana căreia îi aparțin respectivele date să poată fi identificată cu un grad foarte 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 datele dactiloscopice sunt găsite pe o armă sau pe orice obiect utilizat la comiterea infracțiunii. Simpla prezență a datelor dactiloscopice la locul infracțiunii nu ar trebui considerată ca indicând cu un grad foarte ridicat de probabilitate faptul că datele dactiloscopice aparțin autorului acesteia. O altă condiție prealabilă pentru crearea unei astfel de semnalări ar trebui să fie ca identitatea persoanei suspectate să nu poată fi stabilită pe baza datelor provenite din orice altă bază de date relevantă de la nivel național, de la nivelul Uniunii sau de la nivel internațional. Dacă în urma căutării datelor dactiloscopice se identifică o potențială corespondență, statul membru ar trebui să efectueze verificări suplimentare cu participarea experților, pentru a stabili dacă amprentele stocate în SIS aparțin persoanei suspectate, și ar trebui să stabilească identitatea persoanei. Procedura ar trebui să fie reglementată de dreptul intern. O astfel de identificare ar putea contribui în mod substanțial la investigație și ar putea conduce la o arestare, sub rezerva îndeplinirii tuturor condițiilor în vederea arestării.

(24) Ar trebui să se permită căutarea datelor dactiloscopice stocate în SIS cu seturile complete sau incomplete de amprente digitale sau de amprente palmare găsite la locul unei infracțiuni, dacă se poate stabili cu un grad ridicat de probabilitate că aparțin autorului unei infracțiuni grave sau al unei infracțiuni de terorism, cu condiția ca o căutare să fie efectuată simultan în bazele de date naționale relevante de amprente digitale. Ar trebui să se acorde o atenție deosebită stabilirii unor standarde de calitate aplicabile stocării datelor biometrice, inclusiv a datelor dactiloscopice latente.

(25) Ori de câte ori identitatea unei persoane nu poate fi stabilită prin niciun alt mijloc, ar trebui să se utilizeze datele dactiloscopice în încercarea de identificare. Identificarea unei persoane prin utilizarea datelor dactiloscopice ar trebui să fie permisă în toate cazurile.

(26) În cazurile clar definite în care datele dactiloscopice nu sunt disponibile, ar trebui să fie posibil să se adauge un profil ADN la o semnalare. Respectivul profil ADN 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 ascendenților direcți, descendenților sau ale fraților ori surorilor pentru a se putea efectua identificarea. Datele ADN ar trebui să conțină doar minimul de informații necesare pentru identificarea persoanei dispărute.

(27) Profilurile ADN nu ar trebui extrase din SIS decât în cazul în care identificarea este necesară și proporțională în scopurile enunțate în prezentul regulament. Profilurile ADN nu ar trebui extrase sau prelucrate în niciun alt scop decât scopul în care au fost introduse în SIS. Ar trebui să se aplice normele de protecție și de securitate a datelor prevăzute în prezentul regulament. Ar trebui introduse, dacă este necesar, garanții suplimentare atunci când se utilizează profilurile ADN, pentru a se evita riscul de corespondențe false, de piraterie informatică și de partajare neautorizată cu părți terțe.

(28) SIS ar trebui să conțină semnalări referitoare la persoane căutate în vederea arestării în scopul predării și al extrădării. În afară de semnalări, este oportun să se asigure, prin intermediul birourilor SIRENE, schimbul de informații suplimentare care sunt necesare pentru procedurile de predare și de extrădare. În special, ar trebui să fie prelucrate în SIS datele menționate la articolul 8 din Decizia-cadru 2002/584/JAI a Consiliului ([13]). Din motive operaționale, este oportun ca statul membru emitent, cu autorizația autorităților judiciare, să suspende temporar disponibilitatea unei semnalări existente în vederea arestării atunci când o persoană care face obiectul unui mandat european de arestare este căutată în mod intens și activ, iar 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, în principiu, să depășească 48 de ore.

(29) 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.

(30) SIS ar trebui să conțină semnalări referitoare la persoane dispărute sau vulnerabile care trebuie împiedicate să călătorească pentru a li se asigura protecția sau pentru a se preîntâmpina amenințările la adresa siguranței publice sau ordinii publice. În cazul copiilor, aceste semnalări și procedurile corespunzătoare ar trebui să servească interesul superior al copilului, în conformitate cu articolul 24 din Carta drepturilor fundamentale a Uniunii Europene și cu articolul 3 din Convenția Organizației Națiunilor Unite cu privire la drepturile copilului din 20 noiembrie 1989. În urma unei semnalări referitoare la un copil, autoritățile competente, inclusiv cele judiciare, ar trebui să întreprindă acțiuni și să ia decizii în cooperare cu autoritățile de protecție a copilului. După caz, ar trebui informată linia telefonică națională de urgență pentru copii dispăruți.

(31) Semnalările referitoare la persoane dispărute care trebuie plasate sub protecție ar trebui introduse la cererea autorității competente. Toți copiii care au dispărut din centrele de primire ale statelor membre ar trebui să facă obiectul unei semnalări privind persoane dispărute în SIS.

(32) Semnalările referitoare la copiii expuși riscului de răpire de către unul dintre părinți ar trebui introduse în SIS la cererea autorităților competente, inclusiv a autorităților judiciare competente în materia răspunderii părintești, în temeiul dreptului intern. Semnalările referitoare la copiii expuși riscului de răpire de către unul dintre părinți ar trebui introduse în SIS doar în situațiile în care riscul este concret și evident și în circumstanțe limitate. Prin urmare este necesar să se prevadă garanții stricte și adecvate. Atunci când evaluează existența unui risc concret și evident ca un copil să fie scos în mod iminent și ilegal dintr-un stat membru, autoritatea competentă ar trebui să țină cont de situația personală a copilului și de mediul la care acesta este expus.

(33) Prezentul regulament ar trebui să stabilească o nouă categorie de semnalări pentru anumite categorii de persoane vulnerabile care trebuie împiedicate să călătorească. Persoanele care necesită protecție din motive de vârstă, handicap sau situație familială ar trebui considerate vulnerabile.

(34) Ar trebui introduse în SIS semnalări referitoare la copiii care trebuie împiedicați să călătorească pentru propria lor protecție, dacă există un risc concret și evident ca aceștia să fie îndepărtați de pe teritoriul unui stat membru sau să îl părăsească. Ar trebui introduse astfel de semnalări în cazul în care călătoria i-ar expune riscului de a deveni victime ale traficului de ființe umane sau ale căsătoriilor forțate, mutilării genitale feminine sau altor forme de violență de gen, de a deveni victime ale infracțiunilor de terorism sau de a fi implicați în acestea, de a fi recrutați sau înrolați în grupări armate sau de a fi obligați să participe activ la ostilități.

(35) Ar trebui introduse semnalări referitoare la adulții vulnerabili care trebuie împiedicați să călătorească pentru propria lor protecție, în cazul în care călătoria i-ar expune riscului de a deveni victime ale traficului de ființe umane sau ale violenței de gen.

(36) Pentru a oferi garanții stricte și adecvate, semnalările referitoare la copii sau la alte persoane vulnerabile care trebuie împiedicate să călătorească ar trebui, în cazurile în care acest lucru este prevăzut în dreptul intern, să fie introduse în SIS în urma deciziei unei autorități judiciare sau a deciziei unei autorități competente, confirmată de o autoritate judiciară.

(37) Ar trebui să se introducă o nouă acțiune de urmat pentru a permite oprirea și interogarea unei persoane pentru ca statul membru emitent să obțină informații detaliate. Respectiva acțiune ar trebui să se aplice cazurilor în care, pe baza unui indiciu clar, o persoană este suspectată că intenționează să comită sau comite oricare dintre infracțiunile menționate la articolul 2 alineatele (1) și (2) din Decizia-cadru 2002/584/JAI, atunci când sunt necesare mai multe informații pentru executarea unei pedepse cu închisoarea sau a unei măsuri de siguranță privative de libertate a unei persoane condamnate pentru oricare dintre infracțiunile menționate la articolul 2 alineatele (1) și (2) din Decizia-cadru 2002/584/JAI, sau dacă există motive să se creadă că respectiva persoană va comite o astfel de infracțiune. De asemenea, această acțiune de urmat nu ar trebui să aducă atingere mecanismelor de asistență judiciară reciprocă existente. Ea ar trebui să furnizeze suficiente informații pentru a se decide cu privire la acțiuni suplimentare. Această nouă acțiune nu ar trebui să implice nici percheziționarea, nici arestarea respectivei persoane. Drepturile procedurale de care beneficiază persoana suspectată sau acuzată în temeiul dreptului Uniunii sau al dreptului intern ar trebui menținute, inclusiv dreptul acesteia de a avea acces la un avocat în conformitate cu Directiva 2013/48/UE a Parlamentului European și a Consiliului ([14]).

(38) În cazul semnalărilor referitoare la obiecte căutate pentru a fi confiscate sau folosite ca probe în cadrul procedurilor penale, obiectele în cauză ar trebui să fie confiscate în conformitate cu dreptul intern care stabilește dacă și conform căror condiții se confiscă un obiect, mai ales dacă se află în posesia proprietarului său de drept.

(39) SIS ar trebui să conțină noi categorii de obiecte de valoare ridicată, cum ar fi produse din domeniul tehnologiei informației care pot fi identificate și care pot face obiectul unei căutări printr-un număr de identificare unic.

(40)În ceea ce privește semnalările introduse în SIS privind documentele în scopul confiscării sau al folosirii ca probe în cadrul procedurilor penale, termenul „fals” ar trebui înțeles ca referindu-se atât la documentele falsificate, cât și la cele contrafăcute.

(41)Ar trebui să fie posibil ca un stat membru să aplice unei semnalări o mențiune, denumită „indicator de validitate”, care să arate că acțiunea de urmat pe baza semnalării nu va fi întreprinsă pe teritoriul său. În cazul în care semnalările sunt introduse în vederea arestării sau predării, nicio dispoziție a prezentului regulament nu ar trebui interpretată în scopul de a deroga de la dispozițiile Deciziei-cadru 2002/584/JAI sau de a împiedica aplicarea acestora. Decizia de a adăuga un indicator de validitate unei semnalări în scopul neexecutării unui mandat european de arestare ar trebui să se bazeze numai pe motivele de refuz prevăzute în decizia-cadru menționată.

(42)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, locul în care se află persoana ar trebui comunicat întotdeauna autorității judiciare emitente, care poate decide transmiterea unui mandat european de arestare autorității judiciare competente în conformitate cu dispozițiile Deciziei-cadru 2002/584/JAI.

(43)Statele membre ar trebui să poată stabili legături între semnalările din SIS. Stabilirea unor legături între două sau mai multe semnalări nu ar trebui să aibă efect asupra acțiunii de urmat, asupra perioadei de reexaminare a semnalărilor sau asupra drepturilor de acces la semnalări.

(44)Semnalările nu ar trebui păstrate în SIS mai mult timp decât este necesar în vederea îndeplinirii scopurilor specifice în care au fost introduse. Perioadele de reexaminare pentru diferite categorii de semnalări ar trebui să fie adecvate scopului acestora. Semnalările referitoare la obiecte care au legătură cu o semnalare referitoare la o persoană ar trebui păstrate numai atât timp cât este păstrată semnalarea referitoare la persoana respectivă. Deciziile de a păstra semnalări referitoare la persoane ar trebui să se bazeze pe o evaluare individuală cuprinzătoare. Statele membre ar trebui să reexamineze semnalările referitoare la persoane și obiecte în cursul perioadelor de reexaminare prevăzute și ar trebui să întocmească statistici referitoare la numărul de semnalări în cazul cărora s-a prelungit perioada de păstrare.

(45)Introducerea unei semnalări în SIS și prelungirea datei de expirare a valabilității unei semnalări din SIS ar trebui să facă obiectul unei cerințe de proporționalitate care implică examinarea faptului dacă un caz concret este suficient de adecvat, relevant și important pentru a justifica introducerea unei semnalări în SIS. În ceea ce privește infracțiunile de terorism, cazul ar trebui considerat suficient de adecvat, de relevant și de important pentru a justifica o semnalare în SIS. Din motive de siguranță publică sau de securitate națională, statele membre ar trebui să fie autorizate, în mod excepțional, să nu introducă o semnalare în SIS atunci când aceasta este de natură să obstrucționeze cercetările, investigațiile sau procedurile oficiale ori judiciare.

(46)Este necesar să se stabilească norme în ceea ce privește ștergerea semnalărilor. O semnalare ar trebui să fie păstrată numai pe durata necesară îndeplinirii scopului în care a fost introdusă. Având în vedere practicile divergente ale statelor membre privind determinarea momentului în care o semnalare și-a îndeplinit scopul, este oportun să se prevadă criterii detaliate pentru fiecare categorie de semnalări pentru a stabili momentul în care acestea ar trebui să fie șterse.

(47)Integritatea datelor din SIS are o importanță majoră. Prin urmare, ar trebui prevăzute garanții adecvate 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 ar trebui să aplice o procedură uniformă de raportare a incidentelor. Personalul acestora ar trebui să beneficieze de o formare corespunzătoare și să fie informat în legătură cu eventualele infracțiuni și sancțiuni în materie.

(48)Datele prelucrate în SIS și informațiile suplimentare conexe care fac obiectul schimbului în temeiul prezentului regulament nu ar trebui transferate sau puse la dispoziția țărilor terțe sau a organizațiilor internaționale.

(49)Este oportun să se acorde acces la SIS serviciilor responsabile cu înmatricularea vehiculelor, a ambarcațiunilor și a aeronavelor pentru a le permite să verifice dacă mijlocul de transport în cauză este căutat deja în statele membre pentru a fi confiscat. De asemenea, este oportun să se acorde acces la SIS serviciilor responsabile cu înregistrarea armelor de foc pentru a le permite să verifice dacă arma de foc în cauză este căutată într-un stat membru pentru a fi confiscată sau dacă există o semnalare referitoare la persoana care solicită înregistrarea.

(50)Accesul direct la SIS ar trebui acordat numai serviciilor publice competente. Acest acces ar trebui să se limiteze la semnalările privind respectivele mijloace de transport și certificatul ori plăcuța lor de înmatriculare sau privind armele de foc și persoanele care solicită înregistrarea. Orice rezultat pozitiv în SIS ar trebui raportat de aceste servicii organelor de poliție, care ar trebui să ia măsuri suplimentare în conformitate cu semnalarea specifică din SIS și vor notifica statul membru emitent cu privire la rezultatul pozitiv prin intermediul birourilor SIRENE.

(51)Fără a aduce atingere normelor mai specifice prevăzute în prezentul regulament, actele cu putere de lege și actele administrative naționale adoptate în temeiul Directivei (UE) 2016/680 ar trebui să se aplice prelucrării, inclusiv colectării și comunicării datelor cu caracter personal în temeiul prezentului regulament de către autoritățile naționale competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor de terorism ori a altor infracțiuni grave ori al executării pedepselor. Accesul la datele introduse în SIS și dreptul de a efectua căutări în aceste date al autorităților naționale competente care sunt responsabile de prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor de terorism sau a altor infracțiuni grave ori de executarea pedepselor fac obiectul tuturor dispozițiilor relevante din prezentul regulament și al celor din Directiva (UE) 2016/680, astfel cum

au fost transpuse în dreptul intern, și în special al monitorizării de către autoritățile de supraveghere menționate în Directiva (UE) 2016/680.

(52) Fără a aduce atingere normelor mai specifice prevăzute în prezentul regulament în ceea ce privește prelucrarea datelor cu caracter personal, Regulamentul (UE) 2016/679 ar trebui să se aplice prelucrării datelor cu caracter personal de către statele membre în temeiul prezentului regulament, cu excepția cazului în care o astfel de prelucrare este efectuată de către autoritățile naționale competente în scopul prevenirii, investigării, depistării sau urmării penale a infracțiunilor de terorism sau a altor infracțiuni grave.

(53) Regulamentul (UE) 2018/1725 al Parlamentului European și a Consiliului ([15]) ar trebui să se aplice prelucrării datelor cu caracter personal de către instituțiile și organele Uniunii atunci când acestea își exercită responsabilitățile care le revin în temeiul prezentului regulament.

(54) Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului ([16]) ar trebui să se aplice prelucrărilor de date cu caracter personal efectuate de către Europol în temeiul prezentului regulament.

(55) În cazurile în care căutările efectuate în SIS de membrii naționali ai Eurojust și de asistenții acestora indică existența unei semnalări introduse de un stat membru, Eurojust nu poate întreprinde acțiunea solicitată. Prin urmare, Eurojust ar trebui să informeze statul membru în cauză pentru a i se permite să se ocupe de caz.

(56) Atunci când folosesc SIS, autoritățile competente ar trebui să asigure respectarea demnității și a integrității persoanei ale cărei date sunt prelucrate. Prelucrarea datelor cu caracter personal în sensul prezentului regulament nu trebuie să conducă la discriminarea persoanelor din orice motive, cum ar fi sex, rasă sau origine etnică, religie sau convingeri, handicap, vârstă sau orientare sexuală.

(57) În ceea ce privește confidențialitatea, dispozițiile relevante din Statutul funcționarilor Uniunii Europene și din Regimul aplicabil celorlalți agenți ai Uniunii prevăzute în Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului ([17])(denumit în continuare „Statutul funcționarilor”) ar trebui să se aplice funcționarilor sau altor agenți care sunt angajați și își desfășoară activitatea în legătură cu SIS.

(58) Atât statele membre, cât și eu-LISA ar trebui să întrețină planuri de securitate pentru a facilita punerea în aplicare a obligațiilor privind securitatea și ar trebui să coopereze pentru a aborda aspectele legate de securitate dintr-o perspectivă comună.

(59) Autoritățile naționale independente de supraveghere menționate în Regulamentul (UE) 2016/679 și în Directiva (UE) 2016/680 (denumite în continuare „autoritățile de supraveghere”) ar trebui să monitorizeze legalitatea prelucrării datelor cu caracter personal de către statele membre în temeiul prezentului regulament, inclusiv schimbul de informații suplimentare. Autorităților de supraveghere ar trebui să li se acorde resurse suficiente pentru îndeplinirea acestei sarcini. 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. De asemenea, este oportun să se solicite statistici anuale din partea statelor membre.

(60) Autoritățile 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 sistemele naționale din statele membre respective în conformitate cu standardele internaționale de audit. Auditul ar trebui să fie efectuat de autoritățile de supraveghere sau autoritățile 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 autorităților de supraveghere în cauză care ar trebui, prin urmare, să dea instrucțiuni auditorului 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.

(61) Autoritatea Europeană pentru Protecția Datelor ar trebui să monitorizeze activitățile instituțiilor și organelor Uniunii în ceea ce privește prelucrarea datelor cu caracter personal în temeiul prezentului regulament. Autoritatea Europeană pentru Protecția Datelor și autoritățile de supraveghere ar trebui să coopereze în cadrul activităților de monitorizare a SIS.

(62) Autoritatea Europeană pentru Protecția Datelor ar trebui să beneficieze de resurse suficiente pentru a-și îndeplini sarcinile care i-au fost încredințate în temeiul prezentului regulament, inclusiv de asistență din partea unor persoane cu expertiză în domeniul datelor biometrice.

(63) Regulamentul (UE) 2016/794 prevede că Europol susține și consolidează acțiunile întreprinse de autoritățile naționale competente 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 referitoare la persoane dispărute ar trebui să îmbunătățească și mai mult capacitatea acestuia de a furniza autorităților naționale de aplicare a legii produse operaționale și analitice cuprinzătoare privind traficul de persoane și exploatarea sexuală a copiilor, inclusiv în mediul online. Aceasta ar contribui la o mai bună prevenire a respectivelor infracțiuni, la protecția potențialelor victime și la investigarea autorilor infracțiunilor. Centrul european de combatere a criminalității informatice din cadrul Europol ar beneficia la rândul său de accesul acordat Europol la semnalările referitoare la persoane dispărute, inclusiv în cazurile autorilor itineranți ai unor infracțiuni sexuale și în cele de abuz sexual asupra copiilor în mediul online, în care autorii infracțiunilor susțin adeseori că au acces sau pot avea acces la copii care ar putea să fi fost înregistrați ca dispăruți.

(64) În vederea eliminării lacunelor în privința schimbului de informații privind terorismul, în special privind luptătorii teroriști străini, ale căror deplasări este extrem de important să fie monitorizate, statele membre sunt încurajate să facă schimb de informații cu Europol privind activitățile legate de terorism. Acest schimb de informații ar trebui să se desfășoare prin intermediul unui schimb de informații suplimentare cu Europol cu privire la semnalările în cauză. În acest scop, Europol ar trebui să creeze o conexiune cu

infrastructura de comunicații.

(65) Este necesar, de asemenea, să se stabilească norme clare privind prelucrarea și descărcarea datelor din SIS de către Europol pentru a se permite o utilizare 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 introduse de un stat membru, Europol nu poate întreprinde acțiunea necesară. Prin urmare, acesta ar trebui să informeze statul membru în cauză printr-un schimb de informații suplimentare cu biroul SIRENE corespunzător, pentru a permite statului membru respectiv să se ocupe de caz.

(66) Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului ([18]) prevede, în sensul regulamentului respectiv, că statul membru gazdă îi autorizează pe membrii echipelor menționate la articolul 2 punctul 8 din regulamentul respectiv, trimise de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă, să consulte bazele de date ale Uniunii, în cazul în care această consultare este necesară pentru îndeplinirea obiectivelor operative specificate în planul operativ privind verificările la frontieră, supravegherea frontierelor și returnarea. 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 menționate la articolul 2 punctele 8 și 9 din regulamentul respectiv este de a oferi întăriri tehnice și operative statelor membre solicitante, în special celor care se confruntă cu provocări disproporționate legate de migrație. Pentru ca echipele menționate la articolul 2 punctele 8 și 9 din regulamentul respectiv să își îndeplinească sarcinile, acestea au nevoie de 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 în SIS efectuate de echipele menționate la articolul 2 punctele 8 și 9 din Regulamentul (UE) 2016/1624 sau de echipele formate din personal indică existența unei semnalări introduse 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, statul membru gazdă ar trebui să fie informat pentru a i se permite să se ocupe de caz. Statul membru gazdă ar trebui să notifice statul membru emitent cu privire la rezultatul pozitiv printr-un schimb de informații suplimentare.

(67) 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 prin prezentul regulament. Aceste aspecte includ, de exemplu, normele tehnice privind introducerea, actualizarea, ștergerea datelor și efectuarea de căutări în acestea și privind calitatea datelor și normele referitoare la datele biometrice, normele privind compatibilitatea și ordinea priorității semnalărilor, privind legăturile dintre semnalări, stabilirea datei de expirare a valabilității semnalărilor în termenul maxim și privind schimbul de informații suplimentare. Prin urmare, ar trebui să i se confere Comisiei 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.

(68) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, ar trebui conferite competențe de executare Comisiei. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([19]). Procedura de adoptare a actelor de punere în aplicare în temeiul prezentului regulament și al Regulamentului (UE) 2018/1861 ar trebui să fie aceeași.

(69) Pentru a se asigura transparența, eu-LISA ar trebui să elaboreze, la doi ani după punerea în funcțiune a SIS în temeiul prezentului regulament, un raport referitor la funcționarea tehnică a SIS central și a infrastructurii de comunicații, inclusiv în ceea ce privește securitatea acestora, și la schimbul bilateral și multilateral de informații suplimentare. Comisia ar trebui să efectueze o evaluare globală din patru în patru ani.

(70) Pentru a asigura buna funcționare a SIS, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui să fie delegată Comisiei în ceea ce privește noile subcategorii de obiecte care urmează să fie căutate pe baza semnalărilor referitoare la obiecte căutate pentru a fi confiscate sau folosite ca probe în cadrul procedurilor penale și determinarea situațiilor în care se pot utiliza fotografii și imagini faciale pentru identificarea persoanelor în alte contexte decât la punctele obișnuite de trecere a frontierei. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare ([20]). În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(71) Întrucât obiectivele prezentului regulament, și anume instituirea și reglementarea unui sistem de informații al Uniunii și schimbul de informații suplimentare conexe, nu pot fi realizate în mod satisfăcător de statele membre, dar, având în vedere natura lor, acestea pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană (TUE). În conformitate cu principiul proporționalității, astfel cum este enunțat la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru atingerea acestor obiective.

(72) Prezentul regulament respectă drepturile fundamentale și principiile recunoscute în special în Carta drepturilor fundamentale a Uniunii Europene. În special, prezentul regulament respectă pe deplin protecția datelor cu caracter personal în conformitate cu articolul 8 din Carta drepturilor fundamentale a Uniunii Europene, vizând în același timp să asigure un mediu sigur pentru toate persoanele care își au reședința pe teritoriul Uniunii și o protecție specială pentru copiii care ar putea cădea victimă traficului de persoane sau răpirii. În cazurile care privesc copii, interesul superior al copilului ar trebui să primeze.

(73) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la TUE și la TFUE, Danemarca nu

participă la adoptarea prezentului regulament, acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică. Deoarece prezentul regulament constituie o dezvoltare a acquis-ului Schengen, Danemarca decide, în conformitate cu articolul 4 din protocolul respectiv, în termen de șase luni de la data la care Consiliul decide cu privire la prezentul regulament dacă îl va pune în aplicare în legislația sa națională.

(74) Regatul Unit participă la prezentul regulament, în conformitate cu articolul 5 alineatul (1) din Protocolul nr. 19 privind acquis-ul Schengen integrat în cadrul Uniunii Europene, anexat la TUE și la TFUE, și cu articolul 8 alineatul (2) din Decizia 2000/365/CE a Consiliului ([21]).

(75) Irlanda participă la prezentul regulament, în conformitate cu articolul 5 alineatul (1) din Protocolul nr. 19 anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, și cu articolul 6 alineatul (2) din Decizia 2002/192/CE a Consiliului ([22]).

(76) În ceea ce privește Islanda și Norvegia, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul 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 ([23]), care se află sub incidența articolului 1 punctul G din Decizia 1999/437/CE a Consiliului ([24]).

(77) În ceea ce privește Elveția, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Acordului între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană cu privire la asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen ([25]), care se află sub incidența articolului 1 punctul G din Decizia 1999/437/CE a Consiliului, coroborat cu articolul 3 din Decizia 2008/149/JAI a Consiliului ([26]).

(78) În ceea ce privește Liechtenstein, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Protocolului între Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în practică, aplicarea și dezvoltarea acquis-ului Schengen ([27]), care se află sub incidența articolului 1 punctul G din Decizia 1999/437/CE, coroborat cu articolul 3 din Decizia 2011/349/UE a Consiliului ([28]).

(79) În ceea ce privește Bulgaria și România, prezentul regulament constituie un act care se întemeiază pe acquis-ul Schengen sau care se raportează la acesta în înțelesul articolului 4 alineatul (2) din Actul de aderare din 2005 și ar trebui coroborat cu Deciziile 2010/365/UE ([29]) și (UE) 2018/934 ([30]) ale Consiliului.

(80) În ceea ce privește Croația, prezentul regulament constituie un act care se întemeiază pe acquis-ul Schengen sau care se raportează la acesta în înțelesul articolului 4 alineatul (2) din Actul de aderare din 2011 și ar trebui coroborat cu Decizia (UE) 2017/733 a Consiliului ([31]).

(81) În ceea ce privește Cipru, prezentul regulament constituie un act care se întemeiază pe acquis-ul Schengen sau care se raportează la acesta în înțelesul articolului 3 alineatul (2) din Actul de aderare din 2003.

(82) 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 cazul acestui stat.

(83) Prezentul regulament introduce o serie de îmbunătățiri în SIS care vor spori eficacitatea acestuia, vor consolida protecția datelor și vor extinde drepturile de acces. O parte a respectivelor îmbunătățiri nu necesită dezvoltări tehnice complexe, în timp ce altele necesită modificări tehnice de diferite dimensiuni. Pentru a permite ca îmbunătățirile aduse sistemului să fie disponibile pentru utilizatorii finali cât mai rapid posibil, prezentul regulament introduce modificări ale Deciziei 2007/533/JAI în mai multe etape. O serie de îmbunătățiri aduse sistemului ar trebui să se aplice imediat după intrarea în vigoare a prezentului regulament, iar altele ar trebui să se aplice după unu sau doi ani de la intrarea în vigoare a acestuia. Prezentul regulament ar trebui să se aplice integral în termen de trei ani de la data intrării sale în vigoare. Pentru a evita întârzierile în aplicarea sa, punerea în aplicare pe etape a prezentului regulament ar trebui să fie monitorizată îndeaproape.

(84) Regulamentul (CE) nr. 1986/2006 al Parlamentului European și al Consiliului ([32]), Decizia 2007/533/JAI și Decizia 2010/261/UE a Comisiei ([33]) ar trebui abrogate de la data aplicării integrale a prezentului regulament.

(85) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ([34]) și a emis un aviz la 3 mai 2017,

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I
Dispoziții generale

Articolul 1

Scopul general al SIS

Obiectivul 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 asigura aplicarea dispozițiilor părții a treia titlul V capitolul 4 și capitolul 5 din TFUE referitoare la circulația persoanelor pe teritoriile statelor membre, folosind informațiile transmise prin intermediul acestui sistem.

Articolul 2

Obiectul

(1) Prezentul regulament stabilește condițiile și procedurile referitoare la introducerea și prelucrarea semnalărilor în SIS referitoare la persoane și obiecte, precum și la schimbul de informații suplimentare și de date suplimentare în scopul cooperării judiciare și polițienești în materie penală.

(2) Prezentul regulament stabilește de asemenea dispoziții privind arhitectura tehnică a SIS, privind responsabilitățile statelor membre și ale Agenției Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA), privind prelucrarea datelor, privind drepturile persoanelor vizate și privind răspunderea.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1.„semnalare” înseamnă un set de date introduse în SIS care permit autorităților competente să identifice o persoană sau un obiect în vederea întreprinderii unei acțiuni specifice;

2.„informații suplimentare” înseamnă informații care nu fac parte din datele semnalării stocate în SIS, dar au legătură cu semnalările din SIS, și care urmează a fi transmise prin intermediul birourilor SIRENE:

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

(b) pentru a permite acțiunea de urmat corespunzătoare în urma obținerii unui rezultat pozitiv;

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

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

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

(f) în ceea ce privește drepturile de acces;

3.„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 efectuării unei căutări în SIS;

4.„date cu caracter personal” înseamnă date cu caracter personal astfel cum sunt definite la articolul 4 punctul 1 din Regulamentul (UE) 2016/679;

5.„prelucrare a 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, consemnarea într-un registru, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

6. „corespondență” înseamnă parcurgerea următoarelor etape:

(a) un utilizator final a efectuat o căutare în SIS;

(b) căutarea respectivă a indicat o semnalare introdusă în SIS de un alt stat membru; și

(c) datele privind semnalarea din SIS corespund datelor căutării;

7.„rezultat pozitiv” înseamnă orice corespondență care îndeplinește următoarele criterii:

(a)a fost confirmată de către:

(i) utilizatorul final; sau

(ii)autoritatea competentă în conformitate cu procedurile naționale, în cazul în care corespondența în cauză s-a bazat pe compararea datelor biometrice;

și

(b) sunt solicitate acțiuni suplimentare;

8.„indicator de validitate” înseamnă suspendarea validității unei semnalări la nivel național, care poate fi adăugat semnalărilor în

vederea arestării, semnalărilor referitoare la persoane dispărute și persoane vulnerabile și semnalărilor în vederea efectuării de controale discrete, de verificări prin interviu și de controale specifice;

9. „stat membru emitent” înseamnă statul membru care a introdus semnalarea în SIS;

10. „stat membru de executare” înseamnă statul membru care întreprinde sau a întreprins acțiunile necesare în urma obținerii unui rezultat pozitiv;

11. „utilizator final” înseamnă un membru al personalului unei autorități competente autorizat să efectueze căutări în mod direct în CS-SIS, N.SIS sau într-o copie tehnică a acestora;

12. „date biometrice” înseamnă date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice sau fiziologice ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, și anume fotografii, imagini faciale, date dactiloscopice și profilul ADN;

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

14. „imagine facială” înseamnă imagini digitale ale feței, având o rezoluție a imaginii și o calitate suficiente pentru a fi utilizate în stabilirea automatizată de corespondențe biometrice;

15. „profil ADN” înseamnă un cod format din litere sau din cifre care reprezintă un set de caracteristici de identificare a părții necodificate a unui eșantion analizat de ADN uman, și anume structura moleculară specifică din diverse segmente de ADN (loci);

16. „infracțiuni de terorism” înseamnă infracțiunile prevăzute de dreptul intern menționate la articolele 3-14 din Directiva (UE) 2017/541 a Parlamentului European și a Consiliului ([35]) sau infracțiuni echivalente cu acestea în cazul statelor membre care nu au obligații în temeiul directivei respective;

17. „amenințare pentru sănătatea publică” înseamnă o amenințare pentru sănătatea publică astfel cum este definită la articolul 2 punctul 21 din Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului ([36]).

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:

(i) o funcție de asistență tehnică („CS-CIS”) ce conține o bază de date (denumită în continuare „baza de date din SIS”), și care include CS-CIS de rezervă;

(ii) 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, inclusiv cel puțin un N.SIS de rezervă național sau comun; și

(c) o infrastructură de comunicații între CS-SIS, CS-SIS de rezervă și NI-SIS (denumită în continuare „infrastructura de comunicații”) care furnizează o rețea virtuală criptată dedicată datelor din SIS și schimbului de date între birourile SIRENE, astfel cum sunt menționate la articolul 7 alineatul (2).

Un N.SIS, astfel cum este menționat la litera (b), poate conține un fișier de date (denumit în continuare „copie națională”) care conține o copie completă sau parțială a bazei de date SIS. Două sau mai multe state membre pot crea în unul dintre sistemele lor N.SIS o copie care poate fi utilizată în comun de statele membre respective. O astfel de copie comună se consideră ca fiind copia națională a fiecăruia dintre statele membre respective.

Un N.SIS de rezervă comun, astfel cum este menționat la litera (b), poate fi folosit în comun de două sau mai multe state membre. În astfel de cazuri, N.SIS de rezervă comun se consideră ca fiind N.SIS de rezervă al fiecăruia dintre statele membre respective. În vederea asigurării disponibilității neîntrerupte pentru utilizatorii finali, N.SIS și N.SIS de rezervă pot fi folosite simultan.

Statele membre care intenționează să creeze o copie comună sau un N.SIS de rezervă comun care să fie utilizate în comun convin în scris asupra responsabilităților care le revin. Acestea notifică Comisiei înțelegerea lor.

Infrastructura de comunicații sprijină și contribuie la asigurarea disponibilității neîntrerupte a SIS. Aceasta include căi redundante și separate pentru conexiunile dintre CS-SIS și CS-SIS de rezervă și, de asemenea, include căi redundante și separate pentru conexiunile dintre fiecare punct național de acces la rețeaua SIS și CS-SIS și CS-SIS de rezervă.

(2) Statele membre introduc, actualizează, șterg datele din SIS și efectuează căutări în datele respective prin intermediul propriilor N.SIS. Statele membre care utilizează o copie națională parțială sau integrală sau o copie comună parțială sau integrală pun la dispoziție respectiva copie pentru efectuarea de căutări automate pe teritoriul fiecăruia dintre respectivele state membre. Copia națională parțială sau comună conține cel puțin datele enumerate la articolul 20 alineatul (3) literele (a)-(v). Nu este posibilă consultarea fișierelor de date din N. SIS ale altor state membre decât în cazul copiilor comune.

(3) CS-SIS îndeplinește funcțiile de supraveghere tehnică și de administrare și are un CS-SIS de rezervă care poate să asigure toate funcționalitățile CS-SIS principal, în cazul în care respectivul sistem încetează să funcționeze. CS-SIS și CS-SIS de rezervă sunt amplasate în cele două amplasamente tehnice ale eu-LISA.

(4) eu-LISA pune în aplicare soluții tehnice pentru a consolida disponibilitatea neîntreruptă a SIS fie prin funcționarea concomitentă a CS-SIS și a CS-SIS de rezervă, cu condiția ca CS-SIS de rezervă să rămână în măsură să asigure funcționarea SIS în cazul unei încetări a funcționării CS-SIS, fie prin duplicarea sistemului sau a componentelor acestuia. În pofida cerințelor procedurale prevăzute la articolul 10 din Regulamentul (UE) 2018/1726, cel târziu până la data de 28 decembrie 2019, eu-LISA pregătește un studiu privind opțiunile în materie de soluții tehnice, incluzând o evaluare independentă a impactului și o analiză cost-beneficiu.

(5) În cazul în care este necesar, în circumstanțe excepționale, eu-LISA poate crea temporar o copie suplimentară a bazei de date din SIS.

(6) CS-SIS furnizează serviciile necesare pentru introducerea datelor în SIS și prelucrarea acestora, inclusiv pentru căutările în baza de date din SIS. Pentru statele membre care utilizează o copie națională sau o copie comună, CS-SIS asigură:

(a) actualizări online ale copiilor naționale;

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

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

(7) CS-SIS asigură disponibilitate neîntreruptă.

Articolul 5

Costuri

(1) Costurile aferente funcționării, întreținerii și dezvoltării în continuare a SIS central și a infrastructurii de comunicații se suportă din bugetul general al Uniunii. Costurile respective includ lucrările care vizează CS-SIS, pentru a asigura furnizarea serviciilor menționate la articolul 4 alineatul (6).

(2) 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 propriului N.SIS și cu conectarea acestuia la NI-SIS.

Fiecare stat membru este responsabil cu asigurarea disponibilității neîntrerupte a datelor din SIS pentru utilizatorii finali.

Fiecare stat membru transmite semnalările sale prin intermediul propriului N.SIS.

Articolul 7

Oficiul N.SIS II 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 asigura respectarea prezentului regulament. Aceasta este responsabilă să asigure că toate funcționalitățile SIS sunt puse în mod corespunzător la dispoziția utilizatorilor finali.

(2) Fiecare stat membru desemnează o autoritate națională care este operațională 24 de ore pe zi, șapte zile pe săptămână și care asigură schimbul și disponibilitatea tuturor informațiilor suplimentare (biroul SIRENE) în conformitate cu manualul SIRENE. Fiecare birou SIRENE servește drept punct unic de contact pentru statul său membru pentru a schimba informații suplimentare despre semnalări și pentru a facilita întreprinderea acțiunilor necesare atunci când s-au introdus în SIS semnalări referitoare la persoane sau obiecte, iar respectivele persoane sau obiecte au fost localizate ca urmare a unui răspuns pozitiv.

În conformitate cu dreptul intern, fiecare birou SIRENE are acces ușor, direct sau indirect, la toate informațiile naționale relevante, inclusiv la bazele de date naționale și la toate informațiile despre semnalările statului său membru, precum și la consiliere de specialitate, astfel încât să poată răspunde, rapid și în termenele prevăzute la articolul 8, cererilor de informații suplimentare.

Birourile SIRENE coordonează verificarea calității informațiilor introduse în SIS. În acest sens, birourile SIRENE au acces la datele prelucrate în SIS.

(3) Statele membre furnizează eu-LISA detalii cu privire la oficiul lor N.SIS și la biroul lor SIRENE. eu-LISA publică lista oficiilor N.SIS și a birourilor SIRENE, împreună cu lista menționată la articolul 56 alineatul (7).

Articolul 8

Schimbul de informații suplimentare

(1) Schimbul de informații suplimentare se efectuează în conformitate cu dispozițiile manualului SIRENE și utilizând infrastructura de comunicații. Statele membre furnizează resursele tehnice și umane necesare pentru a asigura disponibilitatea continuă și schimbul prompt și eficace de informații suplimentare. În cazul în care infrastructura de comunicații este indisponibilă, statele membre folosesc pentru schimbul de informații suplimentare alte mijloace tehnice securizate în mod corespunzător. În manualul SIRENE se include o listă a mijloacelor tehnice securizate în mod corespunzător.

(2) Informațiile suplimentare se utilizează numai în scopul în care au fost transmise în conformitate cu articolul 64, cu excepția cazului în care s-a obținut în prealabil acordul statului membru emitent pentru alte utilizări.

(3) Birourile SIRENE își îndeplinesc sarcinile în mod rapid și eficient, în special prin formularea unui răspuns la o cerere de informații suplimentare cât mai curând posibil, și nu mai târziu de 12 ore de la primirea cererii. În cazul semnalărilor pentru infracțiuni de terorism și în cazul semnalărilor referitoare la persoane căutate în scopul predării sau al extrădării, precum și în cazul semnalărilor referitoare la copii menționate la articolul 32 alineatul (1) litera (c), birourile SIRENE acționează imediat.

Cererile de informații suplimentare cu prioritate absolută sunt marcate cu indicația „URGENT” în formularele SIRENE, în care se specifică și motivul urgenței.

(4) Comisia adoptă acte de punere în aplicare pentru a stabili norme detaliate referitoare la sarcinile birourilor SIRENE în temeiul prezentului regulament și la schimbul de informații suplimentare, sub forma unui manual intitulat „manualul SIRENE”. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

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 asigura compatibilitatea propriului N.SIS cu SIS central în vederea unei transmiteri prompte și eficace a datelor.

(2) În cazul în care un stat membru utilizează o copie națională, acesta se asigură, prin intermediul serviciilor furnizate de CS-SIS și al actualizărilor automate menționate la articolul 4 alineatul (6), că datele stocate în copia națională sunt identice și coerente cu baza de date din SIS și că în urma efectuării unei căutări în copia sa națională se obține un rezultat echivalent cu cel generat de căutarea în baza de date din SIS.

(3) Utilizatorii finali primesc datele necesare pentru îndeplinirea sarcinilor care le revin, în special, și dacă este necesar, toate datele disponibile care permit identificarea persoanei vizate și acțiunea de urmat solicitată.

(4) Statele membre și eu-LISA efectuează teste periodice pentru a verifica conformitatea tehnică a copiilor naționale menționate la alineatul (2). Rezultatele respectivelor teste sunt luate în considerare ca parte a mecanismului instituit prin Regulamentul (UE) nr. 1053/2013 al Consiliului [37].

(5) Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea standardelor, protocoalelor și procedurilor tehnice comune menționate la alineatul (1) din prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

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 utilizatorilor);

(f)a împiedica prelucrarea neautorizată de date în SIS și modificarea sau ștergerea neautorizată a datelor prelucrate în SIS (controlul introducerii datelor);

(g)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 elemente individuale și unice de identificare a utilizatorului și cu folosirea exclusivă a unor moduri de acces confidențiale (controlul accesului la date);

(h)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, să șteargă datele și să efectueze căutări în acestea și că pun fără întârziere respectivele profiluri la dispoziția autorităților de supraveghere menționate la articolul 69 alineatul (1), la cererea acestora (profilurile membrilor personalului);

(i)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);

(j)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 (controlul introducerii);

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

(l)a monitoriza eficacitatea măsurilor de securitate menționate la prezentul alineat și a lua măsurile organizaționale necesare referitoare la monitorizarea internă pentru a asigura respectarea prezentului regulament (auditul intern);

(m) a se asigura că, în cazul unei întreruperi, sistemele instalate pot fi readuse la operarea normală (recuperare); și

(n)a se asigura că SIS își îndeplinește funcțiile corect, că defecțiunile sunt raportate (fiabilitate) și că datele cu caracter personal

stocate în SIS nu pot fi corupte în cazul unei defectări a sistemului (integritate).

(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 prin securizarea sediilor birourilor SIRENE.

(3) Statele membre iau măsuri echivalente celor menționate la alineatul (1) din prezentul articol în materie de securitate în ceea ce privește prelucrarea datelor din SIS de către autoritățile menționate la articolul 44.

(4) Măsurile descrise la alineatele (1), (2) și (3) pot face parte dintr-o abordare și dintr-un plan de securitate generice la nivel național care înglobează mai multe sisteme informatice. În astfel de cazuri, cerințele prevăzute la prezentul articol și aplicabilitatea acestora în ceea ce privește SIS trebuie să fie clar identificabile și asigurate de planul respectiv.

Articolul 11

Confidențialitatea – Statele membre

(1) Fiecare stat membru aplică propriile norme privind secretul profesional sau alte obligații echivalente de confidențialitate pentru toate persoanele și organismele care lucrează cu date din SIS și cu informații suplimentare, în conformitate cu dreptul său intern. Această obligație se aplică și după ce persoanele respective au încetat să mai ocupe o anumită funcție sau un anumit post ori după încetarea activității organismelor respective.

(2) Dacă un stat membru colaborează cu contractanți externi în cadrul oricăror sarcini legate de SIS, acesta monitorizează îndeaproape activitățile contractanților pentru a asigura respectarea tuturor dispozițiilor prezentului regulament, în special cele referitoare la securitate, la confidențialitate și la protecția datelor.

(3) Gestionarea operațională a N.SIS sau a copiilor tehnice nu se încredințează societăților private și nici organizațiilor private.

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 propriul N.SIS în scopul verificării legalității căutării, al monitorizării legalității prelucrării datelor, al automonitorizării și al asigurării funcționării corespunzătoare a N.SIS, precum și a integrității și securității datelor. Această cerință nu se aplică prelucrărilor automate menționate la articolul 4 alineatul (6) literele (a), (b) și (c).

(2) Înregistrările arată, în special, istoricul semnalării, ziua și ora activității de prelucrare a datelor, datele utilizate pentru efectuarea unei căutări, o mențiune cu privire la datele prelucrate și elementele individuale și unice de identificare a utilizatorului, atât ale autorității competente, cât și ale persoanei care prelucrează datele.

(3) Prin derogare de la alineatul (2) din prezentul articol, în cazul în care căutarea se efectuează cu ajutorul datelor dactiloscopice sau al unei imagini faciale în conformitate cu articolul 43, înregistrările arată tipul de date utilizate în locul datelor propriu-zise pentru efectuarea căutării.

(4) Înregistrările se pot utiliza numai în scopurile menționate la alineatul (1) și se șterg la trei ani de la creare. Înregistrările care includ istoricul semnalărilor se șterg la trei ani de la ștergerea semnalărilor.

(5) Înregistrările se pot păstra mai mult timp decât perioadele menționate la alineatul (4) dacă sunt necesare pentru proceduri de monitorizare care se află deja în curs.

(6) Autoritățile naționale competente responsabile cu verificarea legalității căutărilor, cu monitorizarea legalității prelucrării datelor, cu automonitorizarea și cu asigurarea funcționării corespunzătoare a N.SIS și a integrității și securității datelor au acces la înregistrări, în limitele competențelor lor și la cererea acestora, în scopul îndeplinirii atribuțiilor care le revin.

(7) În cazul în care, în conformitate cu dreptul intern, statele membre efectuează căutări automate prin scanarea plăcuțelor de înmatriculare ale autovehiculelor, utilizând sistemele de recunoaștere automată a plăcuțelor de înmatriculare, acestea păstrează înregistrările căutărilor în conformitate cu dreptul intern. Dacă este necesar, se poate efectua o căutare completă în SIS pentru a verifica dacă s-a obținut un rezultat pozitiv. Alineatele (1)-(6) se aplică oricărei căutări complete.

(8) Comisia adoptă acte de punere în aplicare pentru stabilirea conținutului înregistrării menționate la alineatul (7) din prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

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 de supraveghere.

Articolul 14

Formarea personalului

(1) Înainte de a fi autorizat să prelucreze datele stocate în SIS și periodic după acordarea accesului la datele din SIS, personalul autorităților care au drept de acces la SIS beneficiază de o formare corespunzătoare privind securitatea datelor, privind drepturile fundamentale, inclusiv protecția datelor, și privind normele și procedurile referitoare la prelucrarea datelor, astfel cum sunt prevăzute în manualul SIRENE. Personalul este informat despre toate dispozițiile relevante referitoare la infracțiuni și sancțiuni, inclusiv cele prevăzute în articolul 73.

(2) Statele membre dispun de un program național de formare cu privire la SIS, care include formarea utilizatorilor finali, precum și a personalului birourilor SIRENE.

Respectivul program de formare poate face parte dintr-un program general de formare la nivel național care include formarea în alte domenii relevante.

(3) La nivelul Uniunii se organizează cursuri comune de formare cel puțin o dată pe an, pentru a consolida cooperarea între birourile SIRENE.

CAPITOLUL III
Responsabilitățile eu-LISA

Articolul 15

Gestionarea operațională

(1) eu-LISA este responsabilă cu gestionarea operațională a SIS central. În cooperare cu statele membre, eu-LISA se asigură că pentru SIS central se utilizează în permanență cea mai bună tehnologie disponibilă, sub rezerva unei analize cost-beneficiu.

(2) eu-LISA este, de asemenea, responsabilă cu următoarele sarcini legate de infrastructura de comunicații:

(a) supravegherea;

(b) securitatea;

(c) coordonarea relațiilor dintre statele membre și furnizor;

(d) sarcinile aferente execuției bugetare;

(e) achiziții și reînnoire; și

(f) aspecte contractuale.

(3) eu-LISA este, de asemenea, responsabilă cu următoarele sarcini legate de birourile SIRENE și de comunicarea dintre birourile SIRENE:

(a) coordonarea, gestionarea și sprijinirea activităților de testare;

(b)întreținerea și actualizarea specificațiilor tehnice pentru schimbul de informații suplimentare între birourile SIRENE și infrastructura de comunicații; și

(c)gestionarea impactului modificărilor tehnice în cazul în care acestea afectează atât SIS, cât și schimbul de informații suplimentare între birourile SIRENE.

(4) eu-LISA dezvoltă și menține un mecanism și proceduri pentru verificarea calității datelor în CS-SIS. Agenția prezintă rapoarte periodice statelor membre în această privință.

eu-LISA prezintă Comisiei un raport periodic care cuprinde problemele întâmpinate și statele membre în cauză.

Comisia prezintă Parlamentului European și Consiliului un raport periodic cu privire la problemele întâmpinate legate de calitatea datelor.

(5) De asemenea, eu-LISA îndeplinește sarcini legate de formare în privința tehnicilor de utilizare a SIS și a măsurilor de îmbunătățire a calității datelor din SIS.

(6) Gestionarea operațională a SIS central constă în toate sarcinile necesare menținerii SIS central în funcțiune 24 de ore pe zi, șapte zile pe săptămână, în conformitate cu prezentul regulament, în special în activitatea de întreținere și dezvoltările tehnice necesare pentru buna funcționare a sistemului. Respectivele sarcini includ, de asemenea, coordonarea, gestionarea și sprijinirea activităților de testare pentru SIS central și N.SIS, care asigură faptul că SIS central și N.SIS funcționează în conformitate cu cerințele pentru conformitatea tehnică și funcțională stabilite la articolul 9.

(7) Comisia adoptă acte de punere în aplicare pentru a stabili cerințele tehnice referitoare la infrastructura de comunicații. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

Articolul 16

Securitatea – eu-LISA

(1) eu-LISA 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 comunicații 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 utilizatorilor);

(f)a împiedica prelucrarea neautorizată de date în SIS și modificarea sau ștergerea neautorizată a datelor prelucrate în SIS (controlul introducerii datelor);

(g)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 elemente individuale și unice de identificare a utilizatorului și cu folosirea exclusivă a unor moduri de acces confidențiale (controlul accesului la date);

(h)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 respectivele profiluri la dispoziția Autorității Europene pentru Protecția Datelor, la cererea acesteia (profilurile membrilor personalului);

(i)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);

(j)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 (controlul introducerii);

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

(l)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 respectarea prezentului regulament (auditul intern).

(m) a se asigura că, în cazul unor operațiuni întrerupte, sistemele instalate pot fi readuse la operarea normală (recuperare);

(n)a asigura că SIS își îndeplinește funcțiile corect, că defecțiunile sunt raportate (fiabilitate) și că datele cu caracter personal stocate în SIS nu pot fi corupte în cazul unei defectări a sistemului (integritate); și

(o) a asigura securitatea amplasamentelor sale tehnice.

(2) eu-LISA 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 comunicații.

Articolul 17

Confidențialitatea – eu-LISA

(1) Fără a aduce atingere articolului 17 din Statutul funcționarilor, eu-LISA aplică norme corespunzătoare privind secretul profesional sau alte obligații echivalente de confidențialitate, la standarde comparabile cu cele prevăzute la articolul 11 din prezentul regulament, pentru toți membrii personalului său care trebuie să lucreze cu date din SIS. Obligația respectivă 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) eu-LISA ia măsuri echivalente celor menționate la alineatul (1) în materie de confidențialitate în ceea ce privește schimbul de informații suplimentare prin intermediul infrastructurii de comunicații.

(3) Dacă eu-LISA colaborează cu contractanți externi în cadrul oricăror sarcini legate de SIS, aceasta monitorizează îndeaproape activitățile contractanților pentru a asigura respectarea tuturor dispozițiilor prezentului regulament în special cele referitoare la securitate, la confidențialitate și la protecția datelor.

(4) Gestionarea operațională a CS-SIS nu se încredințează societăților private și nici organizațiilor private.

Articolul 18

Păstrarea înregistrărilor la nivel central

(1) eu-LISA 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 prevăzute la articolul 12 alineatul (1).

(2) Înregistrările arată, în special, istoricul semnalării, ziua și ora activității de prelucrare a datelor, datele utilizate pentru efectuarea unei căutări, o mențiune cu privire la datele prelucrate și elementele individuale și unice de identificare a utilizatorului ale autorității competente care prelucrează datele.

(3) Prin derogare de la alineatul (2) din prezentul articol, în cazul în care căutarea se efectuează cu ajutorul datelor dactiloscopice sau al imaginilor faciale în conformitate cu articolul 43, înregistrările arată tipul de date utilizate în locul datelor propriu-zise pentru efectuarea căutării.

(4) Înregistrările se utilizează numai în scopurile menționate la alineatul (1) și se șterg la trei ani de la creare. Înregistrările care includ istoricul semnalărilor se șterg la trei ani de la ștergerea semnalărilor.

(5) Înregistrările se pot păstra mai mult decât perioadele menționate la alineatul (4) dacă sunt necesare pentru proceduri de monitorizare care se află deja în curs.

(6) În scopul automonitorizării și al asigurării funcționării corespunzătoare a CS-SIS, a integrității și securității datelor, eu-LISA are acces la înregistrări în limitele competenței sale.

Autoritatea Europeană pentru Protecția Datelor are acces la respectivele înregistrări la cerere, în limitele competenței sale și în scopul îndeplinirii sarcinilor care îi revin.

CAPITOLUL IV

Informarea publicului

Articolul 19

Campaniile de informare privind SIS

La începutul aplicării prezentului regulament, Comisia, în cooperare cu autoritățile de supraveghere și cu Autoritatea Europeană pentru Protecția Datelor, desfășoară o campanie de informare a publicului despre obiectivele SIS, despre datele stocate în SIS, despre autoritățile care au acces la SIS și despre drepturile persoanelor vizate. Comisia repetă periodic aceste campanii, în cooperare cu autoritățile de supraveghere și cu Autoritatea Europeană pentru Protecția Datelor. Comisia administrează un site internet accesibil publicului care furnizează toate informațiile relevante despre SIS. În cooperare cu propriile autorități de supraveghere, statele membre elaborează și pun în aplicare politicile necesare pentru a asigura informarea generală a cetățenilor și a rezidenților lor despre SIS.

CAPITOLUL V

Categoriile 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 în scopurile prevăzute la articolele 26, 32, 34, 36, 38 și 40.

(2) Categoriile de date sunt următoarele:

(a) informații privind persoanele cu privire la care au fost introduse semnalări;

(b) informații privind obiectele menționate la articolele 26, 32, 34, 36 și 38.

(3) Orice semnalare în SIS care include informații privind persoane conține numai următoarele date:

(a) numele de familie;

(b) prenumele;

(c) numele la naștere;

(d) numele folosite anterior și pseudonimul;

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

(f) locul nașterii;

(g) data nașterii;

(h) genul;

(i) toate cetățeniile deținute;

(j) dacă persoana în cauză:

(i) este înarmată;

(ii) este violentă;

(iii) s-a sustras sau a evadat;

(iv) prezintă un risc de sinucidere;

(v) reprezintă o amenințare pentru sănătatea publică; sau

(vi) este implicată într-o activitate menționată la articolele 3-14 din Directiva (UE) 2017/541;

(k) motivul semnalării;

(l) autoritatea care a creat semnalarea;

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

(n) acțiunea de urmat în cazul unui rezultat pozitiv;

(o) legăturile cu alte semnalări în temeiul articolului 63;

(p) tipul de infracțiune;

(q) numărul de înregistrare al persoanei în cauză într-un registru național;

(r) pentru semnalările menționate la articolul 32 alineatul (1), o clasificare a tipului de caz;

(s) categoria documentelor de identificare ale persoanei;

(t) țara care a eliberat documentele de identificare ale persoanei;

(u) numărul (numerele) documentelor de identificare ale persoanei;

(v) data eliberării documentelor de identificare ale persoanei;

(w) fotografii și imagini faciale;

(x) în conformitate cu articolul 42 alineatul (3), profilurile ADN relevate;

(y) date dactiloscopice;

(z) o copie a documentelor de identificare, color, ori de câte ori este posibil.

(4) Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea normelor tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatele (2) și (3) din prezentul articol, precum și privind efectuarea de căutări în acestea, și a standardelor comune menționate la alineatul (5) din prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

(5) Normele tehnice sunt similare în cazul căutărilor efectuate în CS-SIS, în copiile naționale sau comune și în copiile tehnice efectuate în temeiul articolului 56 alineatul (2). Acestea se bazează pe standarde comune.

Articolul 21

Proporționalitatea

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

(2) În cazul în care se caută o persoană sau un obiect în temeiul unei semnalări legate de o infracțiune de terorism, cazul este considerat suficient de adecvat, de relevant și de important pentru a justifica o semnalare în SIS. Din motive de siguranță publică sau securitate națională, statele membre pot, în mod excepțional, să nu introducă o semnalare atunci când aceasta este de natură să obstrucționeze cercetările, investigațiile sau procedurile oficiale ori judiciare.

Articolul 22

Cerințele privind introducerea unei semnalări

(1) Setul minim de date necesare pentru a introduce o semnalare în SIS sunt datele menționate la articolul 20 alineatul (3) literele (a), (g), (k) și (n), cu excepția situațiilor menționate la articolul 40. Celelalte date menționate la alineatul respectiv sunt introduse la rândul lor în SIS, dacă sunt disponibile.

(2) Datele menționate la articolul 20 alineatul (3) litera (e) din prezentul regulament sunt introduse numai atunci când acest lucru este strict necesar pentru identificarea persoanei în cauză. Atunci când aceste date sunt introduse, statele membre asigură respectarea articolului 10 din Directiva (UE) 2016/680.

Articolul 23

Compatibilitatea semnalărilor

(1) Înainte de a introduce o semnalare, statul membru verifică dacă persoana sau obiectul în cauză face deja obiectul unei semnalări în SIS. Pentru a verifica dacă persoana face deja obiectul unei semnalări, se efectuează și o verificare prin utilizarea datelor dactiloscopice, dacă acestea sunt disponibile.

(2) În SIS se introduce numai o singură semnalare referitoare la o persoană sau la un obiect pentru un stat membru. Dacă este necesar, alte state membre pot introduce noi semnalări referitoare la aceeași persoană sau același obiect, în conformitate cu alineatul (3).

(3) În cazul în care o persoană sau un obiect face deja obiectul unei semnalări în SIS, statul membru care dorește să introducă o nouă semnalare verifică să nu existe nicio incompatibilitate între semnalări. Dacă nu există nicio incompatibilitate, statul membru poate introduce noua semnalare. Dacă semnalările sunt incompatibile, birourile SIRENE ale statelor membre în cauză se consultă printr-un schimb de informații suplimentare pentru a ajunge la un acord. Normele privind compatibilitatea semnalărilor sunt stabilite în manualul SIRENE. În cazul în care anumite interese naționale esențiale impun acest lucru, se pot face derogări de la normele privind compatibilitatea după o consultare între statele membre.

(4) În cazul unor răspunsuri pozitive referitoare la semnalări multiple cu privire la aceeași persoană sau despre același obiect, statul membru de executare respectă normele privind prioritatea semnalărilor stabilite în manualul SIRENE.

În cazul în care o persoană face obiectul unor semnalări multiple introduse de diferite state membre, semnalările în vederea arestării introduse în conformitate cu articolul 26 se execută cu prioritate, sub rezerva articolului 25.

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 articolul 26, 32 sau 36 este incompatibil cu legislația sa internă, cu obligațiile sale internaționale sau cu interesele sale naționale vitale, statul membru respectiv poate solicita adăugarea unui indicator de validitate la semnalare, pentru ca acțiunea de urmat în baza semnalării să nu se desfășoare pe teritoriul său. Indicatorul de validitate se aplică de către biroul SIRENE al statului membru emitent.

(2) Pentru ca statele membre să poată solicita aplicarea unui indicator de validitate unei semnalări introduse în conformitate cu articolul 26, 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 emitent solicită executarea acțiunii, statul membru de executare examinează dacă poate să autorizeze retragerea indicatorului de validitate aplicat la cererea sa. Dacă statul membru de executare este în măsură să facă acest lucru, ia măsurile necesare pentru a se asigura că acțiunea de urmat 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, un stat membru solicită statului membru emitent să adauge un indicator de validitate care împiedică arestarea ca urmare a unei semnalări în vederea arestării în scopul predării atunci când autoritatea judiciară competentă în temeiul dreptului intern 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.

De asemenea, un stat membru poate solicita să se aplice un indicator de validitate semnalării dacă autoritatea sa judiciară competentă eliberează persoana care face obiectul semnalării în timpul procesului de predare.

(2) Cu toate acestea, la cererea unei autorități judiciare competente în temeiul dreptului intern, pe baza unei instrucțiuni generale sau într-un caz specific, un stat membru poate de asemenea solicita statului membru emitent să adauge un indicator de validitate unei semnalări în vederea arestării în scopul predării dacă este evident că executarea mandatului european de arestare va trebui să fie refuzată.

CAPITOLUL VI

Semnalările referitoare la persoane căutate în vederea arestării în scopul predării sau al extrădării

Articolul 26

Obiectivele semnalărilor și condițiile de introducere a acestora

(1) Semnalările referitoare la persoane căutate în vederea arestării în scopul predării pe baza unui mandat european de arestare sau semnalările referitoare la persoane căutate în vederea arestării în scopul extrădării se introduc la cererea autorității judiciare a statului membru emitent.

(2) Semnalările în vederea arestării în scopul predării se introduc de asemenea pe baza mandatelor de arestare emise în conformitate cu acordurile încheiate între Uniune și țările terțe în temeiul tratatelor în scopul predării persoanelor pe baza unui mandat de arestare, care prevăd transmiterea unui astfel de mandat de arestare prin intermediul SIS.

(3) Orice trimitere din prezentul regulament la dispozițiile Deciziei-cadru 2002/584/JAI se interpretează ca incluzând dispozițiile corespunzătoare ale acordurilor încheiate între Uniune și țările terțe în temeiul tratatelor în scopul predării persoanelor pe baza unui mandat de arestare, care prevăd transmiterea unui astfel de mandat de arestare prin intermediul SIS.

(4) În cazul unei operațiuni în curs, statul membru emitent poate să suspende temporar disponibilitatea pentru căutările efectuate de utilizatorii finali din statul membru implicat în operațiune a unei semnalări existente în vederea arestării introduse în conformitate cu prezentul articol. În astfel de cazuri, semnalarea este accesibilă doar birourilor SIRENE. Statele membre suspendă o semnalare numai dacă:

(a) obiectivul operațiunii nu poate fi realizat prin nicio altă măsură;

(b) autoritatea judiciară competentă din statul membru emitent a acordat o autorizație prealabilă; și

(c) toate statele membre implicate în operațiune au fost informate prin schimbul de informații suplimentare.

Funcționalitatea prevăzută la primul paragraf nu se utilizează decât pe o perioadă de maximum 48 de ore. Cu toate acestea, dacă este necesar din punct de vedere operațional, această perioadă poate fi prelungită cu perioade suplimentare de 48 de ore. Statele membre întocmesc statistici referitoare la numărul de semnalări în legătură cu care s-a utilizat această funcționalitate.

(5) Atunci când există indicii clare că obiectele menționate la articolul 38 alineatul (2) literele (a), (b), (c), (e), (g), (h) (j) și (k) au legătură cu o persoană care face obiectul unei semnalări în temeiul alineatelor (1) și (2) din prezentul articol, se pot introduce semnalări referitoare la obiectele respective pentru a se localiza persoana vizată. În aceste cazuri se creează o legătură între semnalarea referitoare la persoană și semnalarea referitoare la obiect, în conformitate cu articolul 63.

(6) Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea normelor necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatul (5) din prezentul articol, precum și privind efectuarea de căutări în acestea. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

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 emitent introduce în SIS o copie a originalului mandatului european de arestare.

Un stat membru poate introduce o copie a mai multor mandate europene de arestare într-o semnalare în vederea arestării în scopul predării.

(2) Statul membru emitent poate introduce o copie a traducerii mandatului european de arestare în una sau mai multe limbi oficiale ale instituțiilor Uniunii.

Articolul 28

Informații suplimentare privind persoane căutate în vederea arestării în scopul predării

Statul membru emitent al unei semnalări în vederea arestării în scopul predării le comunică celorlalte state membre informațiile menționate la articolul 8 alineatul (1) din Decizia-cadru 2002/584/JAI, printr-un schimb de informații suplimentare.

Articolul 29

Informații suplimentare privind persoane căutate în vederea arestării în scopul extrădării

(1) Statul membru emitent al unei semnalări în vederea arestării în scopul extrădării le comunică tuturor celorlalte state membre, printr-un schimb 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 este subiectul semnalării introduse a participat la comiterea infracțiunii;

(e) în măsura în care este posibil, consecințele infracțiunii; și

(f) orice alte informații utile sau necesare pentru executarea semnalării.

(2) Datele menționate la alineatul (1) din prezentul articol 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 de executare.

Articolul 30

Conversia unei acțiuni de urmat cu privire la semnalările în vederea arestării în scopul predării sau al extrădării

Atunci când nu se poate efectua arestarea, deoarece statul membru căruia i s-a solicitat aceasta refuză să o efectueze în conformitate cu procedurile privind aplicarea unui indicator de validitate stabilite la articolul 24 sau 25, sau, în cazul unei semnalări în vederea arestării în scopul extrădării, deoarece investigația nu s-a finalizat, statul membru căruia i s-a solicitat să efectueze arestarea acționează cu privire la semnalare prin comunicarea locului unde se află persoana în cauză.

Articolul 31

Executarea unei acțiuni pe baza unei semnalări în vederea arestării în scopul predării sau al extrădării

(1) O semnalare introdusă în SIS în conformitate cu articolul 26 și datele suplimentare menționate la articolul 27, constituie împreună un mandat european de arestare emis în conformitate cu Decizia-cadru 2002/584/JAI și au același efect ca acesta 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 are aceeași forță juridică 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 referitoare la persoane dispărute sau vulnerabile care trebuie împiedicate să călătorească

Articolul 32

Obiectivele semnalărilor și condițiile de introducere a acestora

(1) Se introduc în SIS semnalări referitoare la următoarele categorii de persoane, la cererea autorității competente a statului membru emitent:

(a) persoane dispărute care trebuie plasate sub protecție:

(i) pentru propria lor protecție;

(ii) pentru a preîntâmpina o amenințare la adresa ordinii publice sau siguranței publice;

(b) persoane dispărute care nu trebuie plasate sub protecție;

(c) copii expuși riscului de răpire de către un părinte, un membru al familiei sau un tutore, care trebuie împiedicați să călătorească;

(d) copii care trebuie împiedicați să călătorească din cauza unui risc concret și evident de a fi îndepărtați de pe teritoriul unui stat membru sau de a părăsi teritoriul unui stat membru și:

(i) de a deveni victime ale traficului de persoane, ale căsătoriilor forțate, ale mutilării genitale feminine ori ale altor forme de violență bazată pe gen;

(ii) de a deveni victime ale infracțiunilor de terorism sau de a fi implicați în acestea; sau

(iii) de a fi recrutați sau înrolați în grupări armate sau de a fi obligați să participe activ la ostilități;

(e) persoane vulnerabile majore și care trebuie împiedicate să călătorească pentru propria lor protecție din cauza unui risc concret și evident de a fi îndepărtate de pe teritoriul unui stat membru sau de a părăsi teritoriul unui stat membru și de a deveni victime ale traficului de persoane sau ale violenței de gen.

(2) Alineatul (1) litera (a) se aplică în special copiilor și persoanelor care trebuie să facă obiectul internării în urma unei decizii emise de o autoritate competentă.

(3) Ca urmare a unei decizii din partea autorităților competente, inclusiv a autorităților judiciare din statele membre competente în materia răspunderii părintești, se introduce o semnalare referitoare la un copil din categoria menționată la alineatul 1 litera (c) atunci când există un risc concret și evident ca respectivul copil să fie îndepărtat ilegal și iminent din statul membru în care sunt situate autoritățile competente.

(4) O semnalare referitoare la persoanele menționate la alineatul (1) literele (d) și (e) se introduce ca urmare a unei decizii din partea autorităților competente, inclusiv a autorităților judiciare.

(5) Statul membru emitent reexaminează periodic necesitatea de a se menține semnalările menționate la alineatul (1) literele (c), (d) și (e) din prezentul articol în conformitate cu articolul 53 alineatul (4).

(6) Statul membru emitent asigură faptul că:

(a) datele pe care le introduce în SIS indică în care dintre categoriile menționate la alineatul (1) se încadrează persoana la care se referă semnalarea;

(b) datele pe care le introduce în SIS indică despre ce tip de caz este vorba, dacă tipul de caz este cunoscut; și

(c) în ceea ce privește semnalările introduse în conformitate cu alineatul (1) literele (c), (d) și (e), biroul său SIRENE are la dispoziție toate informațiile relevante în momentul creării semnalării.

(7) Cu patru luni înainte ca un copil care face obiectul unei semnalări în temeiul prezentului articol să împlinească vârsta majoratului conform dreptului intern al statului membru emitent, CS-SIS notifică automat statului membru emitent că este necesar ca motivul semnalării și acțiunea de urmat să fie actualizate sau ca semnalarea să fie ștearsă.

(8) Atunci când există indicii clare că obiectele menționate la articolul 38 alineatul (2) literele (a), (b), (c), (e), (g), (h) și (k) au legătură cu o persoană care face obiectul unei semnalări în temeiul alineatului (1) din prezentul articol, se pot introduce semnalări referitoare la obiectele respective pentru a se localiza persoana. În aceste

cazuri se creează o legătură între semnalarea referitoare la persoană și semnalarea referitoare la obiect, în conformitate cu articolul 63.

(9) Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea normelor privind clasificarea tipurilor de cazuri și introducerea datelor menționate la alineatul (6). Tipurile de cazuri de persoane dispărute care sunt copii includ, dar nu se limitează la fugari, copii neînsoțiți în contextul migrației și copii expuși riscului de a fi răpiți de către părinți.

Comisia adoptă de asemenea acte de punere în aplicare pentru stabilirea și dezvoltarea normelor tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatul (8), precum și privind efectuarea de căutări în acestea.

Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

Articolul 33

Executarea acțiunii pe baza unei semnalări

(1) Atunci când o persoană care intră sub incidența articolului 32 este localizată, autoritățile competente ale statului membru de executare comunică statului membru emitent unde se află aceasta, sub rezerva cerințelor de la alineatul (4).

(2) În cazul persoanelor care trebuie plasate sub protecție menționate la articolul 32 alineatul (1) literele (a), (c), (d) și (e), statul membru de executare consultă imediat propriile sale autorități competente și pe cele ale statului membru emitent, printr-un schimb de informații suplimentare, pentru a conveni fără întârziere asupra măsurilor care trebuie luate. Autoritățile competente din statul membru de executare pot, în conformitate cu dreptul intern, să transfere astfel de persoane într-un loc sigur pentru a le împiedica să își continue călătoria.

(3) În cazul copiilor, orice decizie privind măsurile care trebuie luate sau orice decizie de transferare a copilului către un loc sigur, astfel cum se menționează la alineatul (2), se ia în funcție de interesul suprem al copilului. Astfel de decizii se iau imediat și într-un interval de maximum 12 ore din momentul în care a fost localizat copilul, în consultare cu autoritățile relevante de protecție a copilului, după caz.

(4) 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 referitoare la persoane căutate în vederea participării la o procedură judiciară

Articolul 34

Obiectivele semnalărilor și condițiile de introducere a acestora

(1) Pentru a comunica locul de reședință sau domiciliul persoanelor, statele membre introduc în SIS, la cererea unei autorități competente, semnalări 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 pentru care sunt urmărite penal;

(c) persoane cărora trebuie să li se notifice sau comunice o hotărâre penală sau alte documente privind o procedură penală pentru a răspunde în legătură cu fapte pentru care sunt urmărite penal;

(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) Atunci când există indicii clare că obiectele menționate la articolul 38 alineatul (2) literele (a), (b), (c), (e), (g), (h) și (k) au legătură cu o persoană care face obiectul unei semnalări în temeiul alineatului (1) din prezentul

articol, se pot introduce semnalări referitoare la obiectele respective pentru a se localiza persoana. În aceste cazuri se creează o legătură între semnalările referitoare la persoană și semnalarea referitoare la obiect, în conformitate cu articolul 63.

(3) Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea normelor tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatul (2) din prezentul articol, precum și privind efectuarea de căutări în acestea. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

Articolul 35

Executarea acțiunii pe baza unei semnalări

Informațiile cerute i se comunică statului membru emitent printr-un schimb de informații suplimentare.

CAPITOLUL IX

Semnalările referitoare la persoane și obiecte în scopul efectuării de controale discrete, de controale prin interviu sau de controale specifice

Articolul 36

Obiectivele semnalărilor și condițiile de introducere a acestora

(1) Semnalările referitoare la persoane, cele referitoare la obiectele menționate la articolul 38 alineatul (2) literele (a), (b), (c), (e), (g), (h), (i), (k) și (l) și cele referitoare la mijloacele de plată fără numerar se introduc în conformitate cu dreptul intern al statului membru emitent, în scopul efectuării de controale discrete, de controale prin interviu sau de controale specifice, în conformitate cu articolul 37 alineatele (3), (4) și (5).

(2) Atunci când introduc semnalări în scopul efectuării de controale discrete, de controale prin interviu sau de controale specifice și în cazul în care informațiile solicitate de statul membru emitent sunt suplimentare celor prevăzute la articolul 37 alineatul (1) literele (a)-(h), statul membru emitent adaugă la semnalare toate informațiile solicitate. Dacă respectivele informații se referă la categoriile speciale de date cu caracter personal menționate la articolul 10 din Directiva (UE) 2016/680, se efectuează căutări în acestea numai dacă acest lucru este strict necesar în scopul specific al semnalării și în legătură cu infracțiunea care a determinat introducerea semnalării.

(3) Semnalările referitoare la persoane în scopul efectuării de controale discrete, de controale prin interviu sau de controale specifice pot fi introduse în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor, al executării unei pedepse și al preîntâmpinării amenințărilor pentru siguranța publică în una sau mai multe dintre următoarele circumstanțe:

(a) atunci când există indicii clare că o persoană intenționează să comită sau comite oricare dintre infracțiunile menționate la articolul 2 alineatele (1) și (2) din Decizia-cadru 2002/584/JAI;

(b) atunci când informațiile menționate la articolul 37 alineatul (1) sunt necesare pentru executarea unei pedepse cu închisoarea sau a unei măsuri de siguranță privative de libertate a unei persoane condamnate pentru oricare dintre infracțiunile menționate la articolul 2 alineatele (1) și (2) din Decizia-cadru 2002/584/JAI;

(c) atunci când, în urma evaluării generale a unei persoane, în special pe baza infracțiunilor pe care le-a comis în trecut, există motive să se creadă că respectiva persoană ar putea comite infracțiunile menționate la articolul 2 alineatele (1) și (2) din Decizia-cadru 2002/584/JAI în viitor.

(4) În plus, semnalările referitoare la persoane în scopul efectuării de controale discrete, de controale prin interviu sau de controale specifice pot fi introduse în conformitate cu dreptul intern, la cererea autorităților responsabile cu securitatea națională, dacă există indicii concrete că informațiile menționate la articolul 37 alineatul (1) sunt necesare pentru a preîntâmpina o amenințare gravă din partea persoanei în cauză sau alte amenințări grave la adresa securității naționale interne sau externe. Statul membru care a introdus semnalarea în conformitate cu prezentul alineat informează celelalte state membre cu privire la o astfel de semnalare. Fiecare stat membru stabilește autoritățile cărora li se transmite această informație. Informația se transmite prin intermediul birourilor SIRENE.

(5) Atunci când există indicii clare că obiectele menționate la articolul 38 alineatul (2) literele (a), (b), (c), (e), (g), (h), (j), (k) și (l) sau mijloacele de plată fără numerar au legătură cu infracțiunile grave menționate la alineatul (3) din prezentul articol sau cu amenințările grave menționate la alineatul (4) din prezentul articol, se pot introduce semnalări referitoare la respectivele obiecte și se pot crea legături între aceste semnalări și cele introduse în conformitate cu alineatele (3) și (4) din prezentul articol.

(6) Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea normelor tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatul (5) din prezentul articol și, de asemenea, a informațiilor suplimentare menționate la alineatul (2) din prezentul articol, precum și privind efectuarea de căutări în acestea. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

Articolul 37

Executarea acțiunii pe baza unei semnalări

(1) În scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice, statul membru de executare colectează și comunică statului membru emitent toate sau unele dintre următoarele informații:

(a) faptul că persoana care face obiectul unei semnalări a fost localizată sau că obiectele menționate la articolul 38 alineatul (2) literele (a), (b), (c), (e), (g), (h), (j), (k) și (l) sau mijloacele de plată fără numerar care fac obiectul unei semnalări au fost localizate;

(b) locul, ora și motivul efectuării controlului sau a verificării;

(c) ruta și destinația călătoriei;

(d) persoanele care însoțesc persoana care face obiectul semnalării sau ocupanții vehiculului, ambarcațiunii ori 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 persoana care face obiectul semnalării;

(e) orice identitate dezvăluită și orice descriere a persoanei care utilizează documentul oficial în alb sau documentul de identitate eliberat care face obiectul semnalării;

(f) obiectele menționate la articolul 38 alineatul (2) literele (a), (b), (c), (e), (g), (h), (j), (k) și (l) sau mijloacele de plată fără numerar utilizate;

(g) obiectele transportate, inclusiv documentele de călătorie;

(h) circumstanțele în care persoana, obiectele menționate la articolul 38 alineatul (2) literele (a), (b), (c), (e), (g), (h), (j), (k) și (l) sau mijloacele de plată fără numerar au fost localizate;

(i) orice alte informații solicitate de statul membru emitent în conformitate cu articolul 36 alineatul (2).

Dacă informațiile menționate la primul paragraf litera (i) din prezentul alineat se referă la categoriile speciale de date cu caracter personal menționate la articolul 10 din Directiva (UE) 2016/680, acestea se prelucrează în conformitate cu condițiile prevăzute la articolul respectiv și numai dacă completează alte date cu caracter personal prelucrate în același scop.

(2) Statul membru de executare comunică informațiile menționate la alineatul (1) litera (e) prin intermediul schimbului de informații suplimentare.

(3) Un control discret cuprinde colectarea discretă de cât mai multe informații dintre cele descrise la alineatul (1) în cursul activităților de rutină derulate de autoritățile competente naționale ale statului membru de executare. Colectarea acestor informații nu afectează caracterul discret al controalelor, iar persoanei care face obiectul semnalării nu i se aduce sub nicio formă la cunoștință existența semnalării.

(4) Un control prin interviu cuprinde un interviu cu persoana, inclusiv pe baza informațiilor sau a întrebărilor specifice adăugate semnalării de statul membru emitent în conformitate cu articolul 36 alineatul (2). Interviul se desfășoară în conformitate cu dreptul intern al statului membru de executare.

(5) În timpul controalelor specifice, persoanele, vehiculele, ambarcațiunile, aeronavele, containerele și obiectele transportate pot fi percheziționate în scopurile menționate la articolul 36. Perchezițiile se efectuează în conformitate cu dreptul intern al statului membru de executare.

(6) În cazul în care dreptul intern al statului membru de executare nu autorizează controalele specifice, acestea se înlocuiesc în respectivul stat membru cu controale prin interviu. În cazul în care dreptul intern al statului membru de executare nu autorizează controalele prin interviu, acestea se înlocuiesc în respectivul stat membru cu controale discrete. Atunci când se aplică Directiva 2013/48/UE, statele membre se asigură că se respectă, în condițiile prevăzute în respectiva directivă, drepturile persoanelor suspectate și acuzate de a avea acces la un avocat.

(7) Alineatul (6) nu aduce atingere obligației statelor membre de a pune la dispoziția utilizatorilor finali informațiile solicitate în temeiul articolului 36 alineatul (2).

CAPITOLUL X

Semnalările referitoare la obiecte căutate pentru a fi confiscate sau folosite ca probe în cadrul procedurilor penale

Articolul 38

Obiectivele semnalărilor și condițiile de introducere a acestora

(1) Statele membre introduc în SIS semnalări privind obiectele căutate pentru a fi confiscate sau pentru a fi folosite ca probe în cadrul procedurilor penale.

(2) Semnalările se introduc cu privire la următoarele categorii de obiecte ușor identificabile:

(a) autovehicule, 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) motoare de aeronave;

(j) arme de foc;

(k) documente oficiale în alb care au fost furate, însușite în mod ilegal, pierdute sau despre care se pretinde că ar astfel de documente, fiind însă false;

(l) documente de identitate eliberate, cum ar fi pașapoarte, cărți de identitate, permise de ședere, documente de călătorie și permise de conducere, care au fost furate, însușite în mod ilegal, pierdute sau anulate ori despre care se pretinde că ar fi astfel de documente, fiind însă false;

(m) certificate sau plăcuțe de înmatriculare ale vehiculelor care au fost furate, însușite în mod ilegal, pierdute sau anulate ori despre care se pretinde că ar fi astfel de documente ori plăcuțe, fiind însă false;

(n) bancnote (bancnote înregistrate) și bancnote false;

(o) articole din domeniul tehnologiei informației;

(p) componente identificabile ale autovehiculelor;

(q) componente identificabile ale echipamentelor industriale;

(r) alte obiecte de mare valoare identificabile, astfel cum sunt definite în conformitate cu alineatul (3).

În ceea ce privește documentele menționate la literele (k), (l) și (m), statul membru emitent poate preciza dacă aceste documente sunt furate, însușite în mod ilegal, pierdute, anulate sau false.

(3) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 75 pentru a modifica prezentul regulament definind noi subcategorii de obiecte în temeiul alineatului (2) literele (o), (p), (q) și (r) din prezentul articol.

(4) Comisia adoptă acte de punere în aplicare pentru a stabili și a dezvolta normele tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatul (2) din prezentul articol și efectuarea de căutări în acestea. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

Articolul 39

Executarea acțiunii pe baza unei semnalări

(1) În cazul în care în urma unei căutări în date se identifică o semnalare referitoare la un obiect care a fost localizat, autoritatea competentă confiscă, în conformitate cu dreptul său intern, obiectul și contactează autoritatea statului membru emitent 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) sunt comunicate printr-un schimb de informații suplimentare.

(3) Statul membru de executare ia măsurile solicitate în conformitate cu dreptul intern.

CAPITOLUL XI

Semnalările referitoare la persoane necunoscute căutate în scopul identificării în temeiul dreptului intern

Articolul 40

Semnalările referitoare la persoane necunoscute căutate în scopul identificării în temeiul dreptului intern

Statele membre pot introduce în SIS semnalări referitoare la persoane necunoscute căutate, care conțin date dactiloscopice. Respectivele date dactiloscopice sunt seturi complete sau incomplete de amprente digitale sau de amprente palmare descoperite la locul comiterii unor infracțiuni de terorism sau al altor infracțiuni grave în curs de investigare. Acestea se introduc în SIS numai dacă se poate stabili cu un grad foarte ridicat de probabilitate că aparțin unui autor al infracțiunii.

Dacă autoritatea competentă a statului membru emitent nu poate stabili identitatea persoanei suspectate pe baza datelor provenite din nicio altă bază de date relevantă de la nivel național, de la nivelul Uniunii sau de la nivel internațional, datele dactiloscopice menționate la primul paragraf pot fi introduse doar în această categorie de semnalări cu mențiunea „persoană căutată necunoscută” în scopul identificării unei astfel de persoane.

Articolul 41

Executarea acțiunii pe baza unei semnalări

În cazul obținerii unui rezultat pozitiv după efectuarea unei căutări în datele introduse în temeiul articolului 40, identitatea persoanei se stabilește în conformitate cu dreptul intern, iar un expert verifică dacă datele dactiloscopice din SIS aparțin respectivei persoane. Statele membre de executare comunică informații despre identitatea și localizarea persoanei statului membru emitent printr-un schimb de informații suplimentare în scopul de a facilita investigarea în timp util a cazului.

CAPITOLUL XII

Norme specifice privind datele biometrice

Articolul 42

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

(1) În SIS se introduc numai fotografiile, imaginile faciale și datele dactiloscopice menționate la articolul 20 alineatul (3) literele (w) și (y) care îndeplinesc standardele minime de calitate a datelor și specificațiile tehnice.

Înainte de introducerea acestor date, se efectuează o verificare a calității pentru a evalua dacă au fost îndeplinite standardele minime de calitate a datelor și specificațiile tehnice.

(2) Datele dactiloscopice introduse în SIS pot consta în una până la zece amprente digitale plane și una până la 10 amprente digitale prelevate prin rulare. Acestea pot include și până la două amprente palmare.

(3) Se poate adăuga un profil ADN la semnalări doar în situațiile prevăzute la articolul 32 alineatul (1) litera (a), numai după o verificare a calității pentru a se stabili dacă au fost îndeplinite standardele minime de calitate a datelor și specificațiile tehnice și numai dacă nu sunt disponibile fotografii, imagini faciale sau date dactiloscopice sau dacă acestea nu permit 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 respective să își dea acordul explicit. În cazul în care un profil ADN este adăugat la o semnalare, acest profil conține informațiile minime strict necesare pentru identificarea persoanei dispărute.

(4) Pentru stocarea datelor biometrice menționate la alineatele (1) și (3) din prezentul articol se stabilesc standarde minime de calitate a datelor și specificații tehnice, în conformitate cu alineatul (5) din prezentul articol. Respectivele standarde minime de calitate a datelor și specificații tehnice stabilesc nivelul de calitate necesar pentru utilizarea datelor cu scopul de a verifica identitatea unei persoanei în conformitate cu articolul 43 alineatul (1) și pentru utilizarea datelor cu scopul de a identifica o persoană în conformitate cu articolul 43 alineatele (2)-(4).

(5) Comisia adoptă acte de punere în aplicare pentru stabilirea standardelor minime de calitate a datelor și a specificațiilor tehnice menționate la alineatele (1), (3) și (4) din prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

Articolul 43

Norme specifice privind verificarea sau efectuarea de căutări prin utilizarea fotografiilor, a imaginilor faciale, a datelor dactiloscopice și a profilurilor ADN

(1) În cazul în care într-o semnalare în SIS sunt disponibile fotografii, imagini faciale, date dactiloscopice și profiluri ADN, astfel de fotografii, imagini faciale, date dactiloscopice și profiluri ADN se utilizează pentru a confirma identitatea unei persoane care a fost localizată în urma unei căutări alfanumerice efectuate în SIS.

(2) Se pot efectua căutări în datele dactiloscopice în orice situație în scopul identificării unei persoane. Cu toate acestea, se efectuează căutări în datele dactiloscopice în scopul identificării în cazul în care identitatea unei persoane nu poate fi stabilită prin niciun alt mijloc În acest scop, SIS central conține un sistem automat de identificare a amprentelor digitale (AFIS).

(3) Se pot efectua căutări în datele dactiloscopice din SIS în legătură cu semnalări introduse în conformitate cu articolele 26, 32, 36 și 40 și prin utilizarea unor seturi complete sau incomplete de amprente digitale sau de amprente palmare descoperite la locul comiterii unor infracțiuni grave sau al unor infracțiuni de terorism în curs de investigare, în cazul în care se poate stabili cu un grad ridicat de probabilitate că respectivele seturi de amprente aparțin unui autor al infracțiunii și cu condiția să se efectueze simultan o căutare în bazele de date dactiloscopice naționale relevante ale statului membru.

(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 în contextul punctelor obișnuite de trecere a frontierei.

Înainte de implementarea acestei funcționalități în SIS, Comisia prezintă un raport care arată dacă tehnologia necesară este disponibilă, gata pentru a fi utilizată și fiabilă. Parlamentul European este consultat în legătură cu raportul.

După începerea utilizării funcționalității la punctele obișnuite de trecere a frontierei, Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 75 pentru a completa prezentul regulament în ceea ce privește stabilirea celorlalte situații în care se pot utiliza fotografii și imagini faciale pentru identificarea persoanelor.

CAPITOLUL XIII
Dreptul de acces și reexaminarea semnalărilor

Articolul 44

Autoritățile naționale competente care au drept de acces la date în SIS

(1) Autoritățile naționale competente au acces la datele introduse în SIS și au dreptul de a efectua căutări în aceste date în mod direct sau într-o copie a bazei de date SIS în următoarele scopuri:

(a) controlul la frontiere, în conformitate cu Regulamentul (UE) 2016/399;

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

(c) prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor de terorism sau a altor infracțiuni grave ori executarea pedepselor în statele membre în cauză, cu condiția ca Directiva (UE) 2018/680 să se aplice;

(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, precum și efectuarea verificărilor asupra resortisanților țărilor terțe care intră ilegal sau care se află în situație de ședere ilegală pe teritoriul statelor membre;

(e) controalele de securitate asupra resortisanților țărilor terțe care solicită protecție internațională, în măsura în care autoritățile care efectuează verificările nu sunt „autorități decizionale" astfel cum sunt definite la articolul 2 litera (f) din Directiva 2013/32/UE a Parlamentului European și a Consiliului ([38]), și, după caz, acordarea de consiliere în conformitate cu Regulamentul (CE) nr. 377/2004 al Consiliului ([39]).

(2) Dreptul de acces la date în SIS și dreptul de a efectua în mod direct căutări în aceste date pot fi exercitate de autoritățile naționale competente responsabile cu acordarea cetățeniei, astfel cum se prevede în dreptul intern, cu scopul de a examina o cerere de acordare a cetățeniei.

(3) 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 autoritățile judiciare naționale, inclusiv cele responsabile cu inițierea urmăririi penale în cadrul procedurilor penale și cu anchetele judiciare anterioare punerii sub acuzare a unei persoane, în îndeplinirea sarcinilor care le revin, astfel cum se prevede în dreptul intern, precum și de către autoritățile lor coordonatoare.

(4) Autoritățile competente menționate la prezentul articol sunt incluse în lista menționată la articolul 56 alineatul (7).

Articolul 45

Serviciile 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 ([40]), au acces la datele introduse în SIS în conformitate cu articolul 38 alineatul (2) literele (a), (b), (c), (m) și (p) din prezentul regulament doar în scopul de a verifica dacă vehiculele, precum și certificatele de înmatriculare și plăcuțele de înmatriculare care le însoțesc, care le sunt prezentate pentru înmatriculare au fost furate, însușite în mod ilegal, pierdute, despre care se pretinde că ar fi astfel de documente ori plăcuțe, fiind însă false, ori dacă sunt căutate pentru a fi folosite ca probe în cadrul unor proceduri penale.

Accesul la date al serviciilor menționate la primul paragraf este reglementat de dreptul intern și 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 date în SIS.

(3) Serviciile menționate la alineatul (1) din prezentul articol care nu sunt servicii publice au dreptul de a accesa date în SIS numai prin intermediul unei autorități menționate la articolul 44. Respectiva 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 autoritate.

(4) Articolul 39 nu se aplică accesului la SIS obținut în conformitate cu prezentul articol. Comunicarea de către serviciile menționate la alineatul (1) din prezentul articol către poliție sau autoritățile judiciare a oricărei informații care a fost obținută prin accesul la SIS este reglementată de dreptul intern.

Articolul 46

Serviciile 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, inclusiv motoarele de aeronave, au acces la următoarele date introduse în SIS în conformitate cu articolul 38 alineatul (2) doar în scopul de a verifica dacă ambarcațiunile, inclusiv motoarele de ambarcațiuni, și aeronavele, inclusiv motoarele de aeronave care le sunt prezentate pentru înmatriculare sau care fac obiectul gestionării traficului au fost furate, însușite în mod ilegal, pierdute ori dacă sunt căutate pentru a fi folosite ca probe în cadrul procedurilor penale:

(a) date privind ambarcațiuni;

(b) date privind motoare de ambarcațiuni;

(c) date privind aeronave;

(d) date privind motoare de aeronave.

Accesul la date al serviciilor menționate la primul paragraf este reglementat de dreptul intern și 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 date în SIS.

(3) Serviciile menționate la alineatul (1) din prezentul articol care nu sunt servicii publice au dreptul de a accesa date în SIS numai prin intermediul unei autorități menționate la articolul 44. Respectiva 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 nu se aplică accesului la SIS obținut în conformitate cu prezentul articol. Comunicarea de către serviciile menționate la alineatul (1) din prezentul articol către poliție sau autoritățile judiciare a oricărei informații care a fost obținută prin accesul la SIS este reglementată de dreptul intern.

Articolul 47

Serviciile de înregistrare a armelor de foc

(1) Serviciile din statele membre responsabile cu eliberarea certificatelor de înregistrare a armelor de foc au drept de acces la datele referitoare la persoane introduse în SIS în conformitate cu articolele 26 și 36 și la datele referitoare la arme de foc introduse în SIS în conformitate cu articolul 38 alineatul (2). Accesul se exercită pentru a verifica dacă persoana care solicită înregistrarea este căutată în vederea arestării în scopul predării sau al extrădării sau în scopul efectuării de controale discrete, de controale prin interviu sau de controale specifice ori pentru a verifica dacă armele de foc prezentate pentru a fi înregistrate sunt căutate pentru a fi confiscate sau pentru a fi folosite ca probe în cursul procedurilor penale.

(2) Accesul la date al serviciilor menționate la alineatul (1) este reglementat de dreptul intern și se limitează la competența specifică a serviciilor în cauză.

(3) Serviciile menționate la alineatul (1) care sunt servicii publice au dreptul de a accesa în mod direct date în SIS.

(4) Serviciile menționate la alineatul (1) care sunt servicii neguvernamentale au acces la date în SIS numai prin intermediul unei autorități menționate la articolul 44. Autoritatea respectivă are dreptul de a accesa datele în mod direct și informează serviciul în cauză dacă arma de foc poate fi înregistrată. Statul membru în cauză se asigură că serviciul respectiv și personalul acestuia sunt obligați să respecte toate restricțiile stabilite în ceea ce privește condițiile de utilizare a datelor care le sunt transmise de către autoritatea intermediară.

(5) Articolul 39 nu se aplică accesului la SIS obținut în conformitate cu prezentul articol. Comunicarea de către serviciile menționate la alineatul (1) din prezentul articol către poliție sau autoritățile judiciare a oricărei informații care a fost obținută datorită accesului la SIS este reglementată de dreptul intern.

Articolul 48

Accesul la date în SIS de către Europol

(1) Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol), instituită prin Regulamentul (UE) 2016/794, are dreptul de a accesa date în SIS și de a efectua căutări în acestea, în cazurile în care acest lucru este necesar pentru îndeplinirea mandatului său. De asemenea, Europol poate face schimb de informații suplimentare și poate solicita informații suplimentare în conformitate cu dispozițiile din manualul SIRENE.

(2) Atunci când o căutare efectuată de Europol indică existența unei semnalări în SIS, Europol informează statul membru emitent printr-un schimb de informații suplimentare, cu ajutorul infrastructurii de comunicații și în conformitate cu dispozițiile prevăzute în manualul SIRENE. Până când Europol va putea utiliza funcționalitățile prevăzute în vederea schimbului de informații suplimentare, acesta informează statul membru emitent prin intermediul canalelor definite de Regulamentul (UE) 2016/794.

(3) Europol poate prelucra informațiile suplimentare pe care i le-au furnizat statele membre pentru a le compara cu bazele sale de date și cu proiectele sale de analiză operațională, în scopul identificării conexiunilor sau a altor legături relevante, precum și pentru analizele strategice, tematice și operaționale menționate la articolul 18 alineatul (2) literele (a), (b) și (c) din Regulamentul (UE) 2016/794. Orice prelucrare de către Europol a informațiilor suplimentare în scopul prezentului articol se efectuează în conformitate cu respectivul regulament.

(4) Utilizarea de către Europol a informațiilor obținute în urma efectuării unei căutări în SIS sau a prelucrării de informații suplimentare este condiționată de acordul statului membru emitent. Dacă statul membru autorizează utilizarea informațiilor respective, tratarea acestora de către Europol intră sub incidența Regulamentului (UE) 2016/794. Europol comunică astfel de informații țărilor terțe și organismelor terțe numai cu acordul statului membru emitent și în deplină conformitate cu dreptul Uniunii în materie de protecție a datelor.

(5) Europol:

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

(b) în pofida articolului 31 alineatul (1) din Regulamentul (UE) 2016/794, șterge informațiile suplimentare care conțin date cu caracter personal cel târziu la un an de la ștergerea semnalării conexe. Prin derogare, în situațiile în care Europol deține, în bazele sale de date sau în cadrul proiectelor sale de analiză operațională, informații cu privire la un caz cu care informațiile suplimentare au legătură, Europol poate, în mod excepțional, pentru a-și putea îndeplini sarcinile, să continue să stocheze informațiile suplimentare atunci când este necesar. Europol informează statul membru emitent și statul membru de executare despre continuarea stocării unor astfel de informații suplimentare și prezintă o motivare în acest sens;

(c) limitează accesul la date în SIS, inclusiv la informațiile suplimentare, la personalul său autorizat în mod expres în acest sens care are nevoie de acces la astfel de date pentru îndeplinirea sarcinilor care îi revin;

(d) adoptă și aplică măsuri menite să asigure securitatea, confidențialitatea și automonitorizarea în conformitate cu articolele 10, 11 și 13;

(e) se asigură că personalul său care este autorizat să prelucreze datele din SIS beneficiază de o formare și de o informare adecvate, în conformitate cu articolul 14 alineatul (1); și

(f) fără a se aduce atingere Regulamentului (UE) 2016/794, permite Autorității Europene pentru Protecția Datelor să monitorizeze și să examineze activitățile pe care le desfășoară Europolul în exercitarea dreptului său de a accesa date în SIS și de a efectua căutări în acestea, precum și în ceea ce privește schimbul de informații suplimentare și prelucrarea acestora.

(6) Europol poate copia date din SIS numai în scopuri tehnice, atunci când respectiva copiere să fie necesară pentru ca personalul Europol autorizat în mod corespunzător să efectueze o căutare directă. Prezentul regulament se aplică și acestor copii. Copia tehnică se utilizează numai pentru stocarea datelor din SIS în timp ce se efectuează căutări în aceste date. După ce s-au efectuat căutări în date, acestea se șterg. 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) În scopul verificării legalității prelucrării datelor, al automonitorizării și al asigurării securității și integrității corespunzătoare a datelor, Europol păstrează înregistrările fiecărei accesări a SIS și fiecărei căutări în SIS în conformitate cu dispozițiile articolului 12. Astfel de înregistrări și documentații nu se consideră a constitui o descărcare sau o copiere ilegală a vreunei părți din SIS.

(8) Statele membre informează Europol printr-un schimb de informații suplimentare ori de câte ori obțin un rezultat pozitiv legat de semnalări referitoare la infracțiuni de terorism. În mod excepțional, statele membre pot să nu informeze Europol în cazul în care informarea acestuia ar pune în pericol investigații în curs sau siguranța unei persoane ori ar fi contrară intereselor esențiale legate de securitatea statului membru emitent.

(9) Alineatul (8) se aplică începând cu data la care Europol este în măsură să primească informații suplimentare în conformitate cu alineatul (1).

Articolul 49

Accesul Eurojust la date în SIS

(1) Numai membrii naționali ai Eurojust și asistenții acestora au dreptul, atunci când este necesar pentru a-și îndeplini mandatul, de a accesa datele în SIS și de a efectua căutări în acestea în limitele mandatului lor, 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, respectivul membru național informează statul membru emitent. Eurojust comunică unor țări terțe și organisme terțe informații obținute în urma unei astfel de căutări numai cu acordul statului membru emitent și în deplină conformitate cu dreptul Uniunii în materie de protecție a datelor.

(3) Prezentul articol nu aduce atingere dispozițiilor Regulamentului (UE) 2018/1727 al Parlamentului European și al Consiliului [41] și ale Regulamentului (UE) 2018/1725 referitoare la protecția datelor și la răspunderea pentru orice prelucrare neautorizată sau incorectă a acestor date de către membrii naționali ai Eurojust sau de asistenții acestora și nici competențelor Autorității Europene pentru Protecția Datelor în temeiul regulamentelor menționate.

(4) În scopul verificării legalității prelucrării datelor, al automonitorizării și al asigurării securității și integrității corespunzătoare a datelor, Eurojust păstrează înregistrările fiecărei accesări a SIS și ale fiecărei căutări în SIS efectuate de un membru național al Eurojust sau de un asistent al acestuia în conformitate cu dispozițiile articolului 12.

(5) Nicio parte a SIS nu se conectează la un sistem 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 și nu se copiază. Înregistrarea accesului și a căutărilor nu se consideră a constitui o descărcare sau o copiere ilegală a datelor din SIS.

(6) Eurojust adoptă și aplică măsuri menite să asigure securitatea, confidențialitatea și automonitorizarea în conformitate cu articolele 10, 11 și 13.

Articolul 50

Accesul la date în SIS de către echipele europene de poliție de frontieră și gardă de coastă, echipele formate din personalul implicat în sarcini legate de returnare și membrii echipelor de sprijin pentru gestionarea migrației

(1) În conformitate cu articolul 40 alineatul (8) din Regulamentul (UE) 2016/1624, membrii echipelor menționate la articolul 2 punctele 8 și 9 din regulamentul respectiv, în conformitate cu mandatele lor respective și cu condiția să fie autorizați să efectueze controale în conformitate cu articolul 44 alineatul (1) din prezentul regulament și să fi beneficiat de formarea necesară în conformitate cu articolul 14 alineatul (1) din prezentul regulament, au dreptul de a accesa date în SIS și de a efectua căutări în acestea, în măsura în care este necesar pentru îndeplinirea sarcinilor ce le revin și în măsura impusă de planul operațional pentru o operațiune specifică. Accesul la date în SIS nu se acordă membrilor altor echipe.

(2) Membrii echipelor menționate la alineatul (1) își exercită dreptul de a accesa date în SIS și de a efectua căutări în acestea în conformitate cu alineatul (1) prin intermediul unei interfețe tehnice. Interfața tehnică este creată și întreținută de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă și permite conectarea directă la SIS central.

(3) Atunci când o căutare efectuată de un membru al echipelor menționate la alineatul (1) din prezentul articol indică existența unei semnalări în SIS, statul membru emitent este informat cu privire la aceasta. În conformitate cu articolul 40 din Regulamentul (UE) 2016/1624, membrii echipelor acționează 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 în care își desfășoară activitatea și, ca regulă generală, în prezența acestora. Statul membru gazdă poate autoriza membrii echipelor să acționeze în numele său.

(4) În scopul verificării legalității prelucrării datelor, al automonitorizării și al asigurării securității și integrității corespunzătoare a datelor, Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă păstrează înregistrările fiecărei accesări a SIS și fiecărei căutări în SIS în conformitate cu dispozițiile articolului 12.

(5) Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă adoptă și aplică măsuri menite să asigure securitatea, confidențialitatea și automonitorizarea în conformitate cu articolele 10, 11 și 13 și se asigură că echipele menționate la alineatul (1) din prezentul articol aplică aceste măsuri.

(6) Nicio dispoziție a prezentului articol nu se interpretează ca aducând atingere dispozițiilor Regulamentului (UE) 2016/1624 în ceea ce privește protecția datelor sau răspunderii Agenției Europene pentru Poliția de Frontieră și Garda de Coastă pentru orice prelucrare neautorizată sau incorectă a datelor de către aceasta.

(7) Fără a aduce atingere alineatului (2), nicio parte a SIS nu se conectează la niciun sistem pentru colectarea și prelucrarea datelor operat de echipele menționate la alineatul (1) sau de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă, iar datele din SIS la care aceste echipe au acces nu se transferă către un astfel de sistem. Nicio parte a SIS nu se descarcă și nu se copiază. Înregistrarea accesului și a căutărilor nu se consideră a constitui o descărcare sau o copiere ilegală a datelor din SIS.

(8) Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă permite Autorității Europene pentru Protecția Datelor să monitorizeze și să examineze activitățile echipelor menționate la prezentul articol în contextul exercitării de către acestea a dreptului de acces la date în SIS și de a efectua căutări în acestea. Aceasta nu aduce atingere altor dispoziții din Regulamentul (UE) 2018/1725.

Articolul 51

Evaluarea utilizării SIS de către Europol, Eurojust și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă

(1) Comisia realizează, cel puțin o dată la cinci ani, o evaluare a funcționării și a utilizării SIS de către Europol, de către membrii naționali ai Eurojust și de asistenții acestora și de către echipele menționate la articolul 50 alineatul (1).

(2) Europol, Eurojust și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă se asigură că se dă curs în mod adecvat constatărilor și recomandărilor care decurg din evaluare.

(3) Un raport cu privire la rezultatele evaluării și la măsurile luate în urma evaluării se transmite Parlamentului European și Consiliului.

Articolul 52

Limitele de acces

Utilizatorii finali, inclusiv Europol, membrii naționali ai Eurojust și asistenții acestora și membrii echipelor menționate la articolul 2 punctele 8 și 9 din Regulamentul (UE) 2016/1624, accesează doar datele care le sunt necesare în scopul îndeplinirii sarcinilor ce le revin.

Articolul 53

Perioada de reexaminare a semnalărilor referitoare la persoane

(1) Semnalările referitoare la persoane se păstrează numai pe durata necesară îndeplinirii scopurilor în care au fost introduse.

(2) Un stat membru poate introduce o semnalare referitoare la o persoană în sensul articolului 26 și al articolului 32 alineatul (1) literele (a) și (b) pentru o perioadă de cinci ani. Statul membru emitent reexaminează necesitatea de a păstra semnalarea în cadrul perioadei de cinci ani.

(3) Un stat membru poate introduce o semnalare referitoare la o persoană în sensul articolelor 34 și 40 pentru o perioadă de trei ani. Statul membru emitent reexaminează necesitatea de a păstra semnalarea în cadrul perioadei de trei ani.

(4) Un stat membru poate introduce o semnalare referitoare la o persoană în sensul articolului 32 alineatul (1) literele (c), (d) și (e) și al articolului 36 pentru o perioadă de un an. Statul membru emitent reexaminează necesitatea de a păstra semnalarea în cadrul perioadei de un an.

(5) Fiecare stat membru stabilește, după caz, perioade de reexaminare mai scurte, în conformitate cu dreptul său intern.

(6) În timpul perioadei de reexaminare menționate la alineatele (2), (3) și (4), statul membru emitent poate decide, în urma unei evaluări individuale cuprinzătoare care se înregistrează, să păstreze semnalarea referitoare la o persoană pentru o perioadă mai lungă decât perioada de reexaminare, dacă acest lucru se dovedește necesar și proporționat pentru scopurile în care a fost introdusă semnalarea. În acest caz, alineatele (2), (3) sau (4) se aplică și prelungirii. Orice astfel de prelungire se comunică CS-SIS.

(7) Semnalările referitoare la persoane se șterg automat după expirarea perioadei de reexaminare menționate la alineatele (2), (3) și (4), cu excepția cazurilor în care statul membru emitent a informat CS-SIS despre o prelungire în temeiul alineatului (6). CS-SIS informează automat statul membru emitent despre ștergerea programată a datelor cu patru luni înainte.

(8) Statele membre întocmesc statistici privind numărul semnalărilor referitoare la persoane ale căror perioade de păstrare au fost prelungite în conformitate cu alineatul (6) din prezentul articol și le transmit, la cerere, autorităților de supraveghere menționate la articolul 69.

(9) De îndată ce devine clar pentru biroul SIRENE că o semnalare privind o persoană și-a atins scopul și ar trebui în consecință să fie ștearsă, acesta notifică imediat autoritatea care a creat semnalarea. Autoritatea are la dispoziție 15 zile calendaristice de la data primirii notificării respective pentru a răspunde că semnalarea a fost ștearsă sau va fi ștearsă ori pentru a motiva păstrarea semnalării. În cazul în care nu a primit nici un răspuns la sfârșitul perioadei de 15 zile, biroul SIRENE se asigură că semnalarea este ștearsă. În cazul în care dreptul intern permite, semnalarea este ștearsă de biroul SIRENE. Birourile SIRENE raportează autorității lor de

supraveghere toate problemele recurente cu care se confruntă atunci când acționează în temeiul prezentului alineat.

Articolul 54

Perioada de reexaminare a semnalărilor referitoare la obiecte

(1) Semnalările referitoare la obiecte se păstrează numai atât timp cât este necesar pentru realizarea scopurilor în care au fost introduse.

(2) Un stat membru poate introduce o semnalare referitoare la obiecte în sensul articolelor 36 și 38 pentru o perioadă de 10 ani. Statul membru emitent reexaminează necesitatea de a menține semnalarea în cadrul perioadei de 10 ani.

(3) Semnalările referitoare la obiecte introduse în conformitate cu articolele 26, 32, 34 și 36 se reexaminează în temeiul articolului 53 în cazurile în care acestea au legătură cu o semnalare referitoare la o persoană. Aceste semnalări se păstrează numai atât timp cât se păstrează semnalarea referitoare la persoană.

(4) În decursul perioadei de reexaminare menționate la alineatele (2) și (3), statul membru emitent poate decide să păstreze semnalarea referitoare la un obiect pentru o perioadă de timp mai lungă decât perioada de reexaminare, atunci când acest lucru se dovedește necesar pentru scopurile în care a fost introdusă semnalarea. În astfel de situații se aplică alineatul (2) sau (3), după caz.

(5) Comisia poate adopta acte de punere în aplicare pentru a stabili perioade de reexaminare mai scurte pentru anumite categorii de semnalări referitoare la obiecte. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

(6) Statele membre întocmesc statistici privind numărul de semnalări referitoare la obiecte a căror perioadă de păstrare a fost extinsă în conformitate cu alineatul (4).

CAPITOLUL XIV
Ștergerea semnalărilor

Articolul 55

Ștergerea semnalărilor

(1) Semnalările în vederea arestării în scopul predării sau al extrădării prevăzute la articolul 26 se șterg atunci când persoana în cauză a fost predată sau extrădată autorităților competente din statul membru emitent. Acestea sunt șterse și atunci când hotărârea judecătorească în temeiul căreia s-a emis semnalarea a fost revocată de autoritatea judiciară competentă în conformitate cu dreptul intern. Acestea sunt șterse, de asemenea, la expirarea semnalării în conformitate cu articolul 53.

(2) Semnalările referitoare la persoanele dispărute sau persoanele vulnerabile care trebuie împiedicate să călătorească în temeiul articolului 32 se șterg în conformitate cu următoarele norme:

(a) în cazul copiilor dispăruți și al copiilor expuși riscului de răpire, semnalarea se șterge:

(i) odată cu soluționarea cazului, de exemplu atunci când copilul a fost localizat sau repatriat ori autoritățile competente din statul membru de executare au adoptat o decizie privind îngrijirea copilului;

(ii) odată cu încetarea valabilității semnalării în conformitate cu articolul 53; sau

(iii) odată cu adoptarea unei decizii de către autoritatea competentă a statului membru emitent;

(b) în cazul adulților dispăruți, dacă nu se solicită măsuri de protecție, semnalarea se șterge:

(i) odată cu executarea acțiunii de urmat, atunci când locul unde se află aceștia este stabilit de statul membru de executare;

(ii) odată cu încetarea valabilității semnalării în conformitate cu articolul 53; sau

(iii) odată cu adoptarea unei decizii de către autoritatea competentă a statului membru emitent;

(c) în cazul adulților dispăruți, dacă se solicită măsuri de protecție, semnalarea se șterge:

(i) odată cu executarea acțiunii de urmat în situația în care persoana este plasată sub protecție;

(ii) odată cu încetarea valabilității semnalării în conformitate cu articolul 53; sau

(iii) odată cu adoptarea unei decizii de către autoritatea competentă a statului membru emitent;

(d)în cazul persoanelor vulnerabile majore care trebuie împiedicate să călătorească pentru propria lor protecție și al copiilor care trebuie împiedicați să călătorească, semnalarea se șterge:

(i) odată cu executarea acțiunii de urmat, cum ar fi plasarea persoanei sub protecție;

(ii) odată cu încetarea valabilității semnalării în conformitate cu articolul 53; sau

(iii) odată cu adoptarea unei decizii de către autoritatea competentă a statului membru emitent.

Fără a aduce atingere dreptului intern, în cazul în care o persoană a fost internată în urma deciziei unei autorități competente, semnalarea poate fi păstrată până la repatrierea respectivei persoane.

(3) Semnalările referitoare la persoane căutate în scopul unei proceduri judiciare în temeiul articolului 34 se șterg:

(a) odată ce locul unde se află persoana a fost comunicat autorității competente a statului membru emitent;

(b) odată cu încetarea valabilității semnalării în conformitate cu articolul 53; sau

(c) odată cu adoptarea unei decizii de către autoritatea competentă a statului membru emitent.

În cazul în care nu se pot întreprinde acțiuni pe baza informațiilor din comunicarea menționată la litera (a), biroul SIRENE al statului membru emitent informează biroul SIRENE al statului membru de executare pentru a soluționa problema.

În situația obținerii unui rezultat pozitiv atunci când datele privind adresa au fost transmise statului membru emitent și un rezultat pozitiv obținut ulterior în același stat membru de executare indică aceleași date privind adresa, rezultatul pozitiv se înregistrează în statul membru de executare, însă nu se retrimit statului membru emitent nici datele privind adresa, nici informații suplimentare. În aceste cazuri, statul membru de executare informează statul membru emitent despre rezultatele pozitive repetate și statul membru emitent efectuează o evaluare individuală cuprinzătoare privind necesitatea de a păstra semnalarea.

(4) Semnalările în scopul efectuării de controale discrete, de controale prin interviu sau de controale specifice prevăzute la articolul 36 se șterg:

(a) odată cu încetarea valabilității semnalării în conformitate cu articolul 53; sau

(b) odată ce autoritatea competentă a statului membru emitent a adoptat o decizie de ștergere a acestora.

(5) Semnalările referitoare la obiecte căutate pentru a fi confiscate sau folosite ca probe în cadrul unor proceduri penale prevăzute la articolul 38 se șterg:

(a)odată cu confiscarea obiectului sau, în cazul unei măsuri echivalente, odată cu efectuarea schimbului necesar ulterior de informații suplimentare între birourile SIRENE implicate sau atunci când obiectul este vizat de o altă procedură judiciară sau administrativă;

(b) odată cu încetarea valabilității semnalării în conformitate cu articolul 53; sau

(c) odată cu adoptarea de către autoritatea competentă a statului membru emitent a unei decizii de ștergere a acestora.

(6) Semnalările referitoare la persoane căutate necunoscute în temeiul articolului 40 se șterg:

(a) odată cu identificarea persoanei;

(b) odată cu încetarea valabilității semnalării în conformitate cu articolul 53; sau

(c) odată cu adoptarea de către autoritatea competentă a statului membru emitent a unei decizii de ștergere a acestora.

(7) În cazurile în care există o legătură cu o semnalare referitoare la o persoană, o semnalare referitoare la un obiect introdusă în conformitate cu articolele 26, 32, 34 și 36 se șterge în momentul în care semnalarea referitoare la persoană se șterge în conformitate cu prezentul articol.

CAPITOLUL XV

Norme generale de prelucrare a datelor

Articolul 56

Prelucrarea datelor din SIS

(1) Statele membre prelucrează 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 sunt copiate numai în scopuri tehnice, atunci când această copiere este necesară pentru ca autoritățile competente menționate la articolul 44 să poată efectua o căutare directă. Prezentul regulament se aplică și respectivelor copii. Un stat membru nu copiază datele dintr-o semnalare 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 menționate la alineatul (2) care generează baze de date offline se pot păstra maximum 48 de ore.

Statele membre țin un inventar actualizat al acestor copii, îl pun la dispoziția autorităților lor de supraveghere și se asigură că prezentul regulament, în special articolul 10, se aplică în cazul acestor copii.

(4) Accesul la date în SIS de către autoritățile naționale competente menționate la articolul 44 este autorizat numai în limitele competențelor acestora și numai personalului autorizat în mod corespunzător.

(5) În ceea ce privește semnalările prevăzute la articolele 26, 32, 34, 36, 38 și 40 din prezentul regulament, orice prelucrare a informațiilor în SIS în alte scopuri decât cele în 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 iminentă și gravă la adresa ordinii publice și siguranței publice, din motive întemeiate de securitate națională sau în scopul prevenirii unei infracțiuni grave. În acest scop, se obține o autorizare prealabilă din partea statului membru emitent.

(6) Orice utilizare a datelor din SIS care contravine alineatelor (1)-(5) din prezentul articol se consideră a fi utilizare abuzivă în temeiul dreptului intern al fiecărui stat membru și face obiectul sancțiunilor în conformitate cu articolul 73.

(7) Fiecare stat membru trimite eu-LISA o listă a autorităților sale competente care sunt autorizate să efectueze în mod direct căutări în date în 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. eu-LISA se asigură că lista este publicată anual în *Jurnalul Oficial al Uniunii Europene*. eu-LISA menține, pe site-ul său, o listă actualizată permanent, care conține modificările transmise de statele membre între publicările anuale.

(8) În măsura în care dreptul Uniunii nu stabilește dispoziții specifice, dreptul fiecărui stat membru se aplică datelor din N.SIS.

Articolul 57

Datele din SIS și fișierele naționale

(1) Articolul 56 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 intern prevăd o perioadă de păstrare mai îndelungată.

(2) Articolul 56 alineatul (2) nu aduce atingere dreptului unui stat membru de a păstra în fișierele sale naționale datele dintr-o anumită semnalare introdusă în SIS de respectivul stat membru.

Articolul 58

Informații în cazul neexecutării unei semnalări

Dacă o acțiune solicitată nu poate fi întreprinsă, statul membru de unde este solicitată acțiunea informează imediat statul membru emitent printr-un schimb de informații suplimentare.

Articolul 59

Calitatea datelor din SIS

(1) Statul membru emitent este responsabil să asigure faptul că datele sunt exacte, actualizate, și introduse și stocate în mod legal în SIS.

(2) În cazul în care un stat membru emitent primește date suplimentare sau modificate relevante, astfel cum sunt enumerate la articolul 20 alineatul (3), acesta completează sau modifică semnalarea în cauză fără întârziere.

(3) Numai statul membru emitent este autorizat să modifice, să completeze, să corecteze, să actualizeze sau să șteargă datele pe care le-a introdus în SIS.

(4) În cazul în care un stat membru, altul decât statul membru emitent, dispune de date modificate sau suplimentare relevante, astfel cum sunt enumerate la articolul 20 alineatul (3), acesta le transmite fără întârziere, printr-un schimb de informații suplimentare, statului membru emitent pentru a îi permite acestuia din urmă să completeze sau să modifice semnalarea. Dacă datele suplimentare sau modificate se referă la persoane, acestea se transmit numai dacă identitatea persoanei este stabilită.

(5) În cazul în care un stat membru, altul decât statul membru emitent, are probe care sugerează că un element al datelor este incorect din punct de vedere factual sau a fost stocat ilegal, respectivul stat membru aduce acest fapt la cunoștința statului membru emitent, printr-un schimb de informații suplimentare, în cel mai scurt timp posibil dar nu mai târziu de două zile lucrătoare de la data la care a descoperit probele respective. Statul membru emitent verifică informațiile și, dacă este necesar, corectează sau șterge imediat elementul în cauză.

(6) În cazul în care statele membre nu ajung la un acord în termen de două luni de la data descoperirii inițiale a probelor, astfel cum se menționează la alineatul (5) din prezentul articol, statul membru care nu a introdus semnalarea sesizează autoritățile de supraveghere competente și Autoritatea Europeană pentru Protecția Datelor în scopul luării unei decizii, prin cooperare în conformitate cu articolul 71.

(7) Statele membre fac schimb de informații suplimentare în situațiile 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 persoana vizată de o semnalare nu este reclamantul, reclamantul este informat cu privire la măsurile prevăzute la articolul 62 și la dreptul la o cale de atac în temeiul articolului 68 alineatul (1).

Articolul 60

Incidente de securitate

(1) Orice eveniment care are sau care poate avea un impact asupra securității SIS sau care poate cauza daune sau pierderi datelor din SIS sau informațiilor suplimentare este considerat a fi un incident de securitate, în special în cazul în care este posibil să se fi accesat în mod ilegal 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) Fără a aduce atingere notificării și comunicării unei încălcări a securității datelor cu caracter personal în temeiul articolului 33 din Regulamentul (UE) 2016/679 sau al articolului 30 din Directiva (UE) 2016/680, statele membre, Europol, Eurojust și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă notifică fără întârziere incidentele de securitate Comisiei, eu-LISA, autorității de supraveghere competente și Autorității Europene pentru Protecția Datelor. eu-LISA notifică fără întârziere Comisiei și Autorității Europene pentru Protecția Datelor orice incident de securitate privind SIS central.

(4) Informațiile referitoare la un incident de securitate care are sau care poate să aibă un impact asupra funcționării SIS într-un stat membru sau în cadrul eu-LISA, asupra disponibilității, a integrității și a confidențialității datelor introduse sau trimise de alte state membre sau asupra informațiilor suplimentare schimbate se pun la dispoziția tuturor statelor membre fără întârziere și se raportează în conformitate cu planul de gestionare a incidentelor furnizat de eu-LISA.

(5) Statele membre și eu-LISA colaborează în cazul unui incident de securitate.

(6) Comisia raportează imediat incidentele grave Parlamentului European și Consiliului. Rapoartele respective se clasifică drept document EU RESTRICTED/RESTREINT UE, în conformitate cu normele de securitate aplicabile.

(7) În cazul în care un incident de securitate este cauzat de utilizarea abuzivă a datelor, statele membre, Europol, Eurojust și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă se asigură că sunt impuse sancțiuni, în conformitate cu articolul 73.

Articolul 61

Diferențierea persoanelor care prezintă caracteristici similare

(1) În cazul în care, la momentul introducerii unei noi semnalări, se constată că există deja o semnalare în SIS referitoare la o persoană cu aceeași descriere a identității, biroul SIRENE contactează în termen de 12 ore statul membru emitent, printr-un schimb de informații suplimentare, pentru a verifica încrucișat dacă subiectele celor două semnalări sunt sau nu aceeași persoană.

(2) În cazul în care verificarea încrucișată arată că persoana care face obiectul noii semnalări şi persoana care face obiectul semnalării deja înregistrate în SIS sunt într-adevăr aceeași persoană, biroul SIRENE aplică procedura privind introducerea de semnalări multiple menționată la articolul 23.

(3) În cazul în care rezultatul verificării încrucișate arată că, de fapt, sunt două persoane diferite, biroul SIRENE aprobă cererea de introducere a celei de a doua semnalări, prin adăugarea datelor necesare pentru a se evita orice identificare eronată.

Articolul 62

Date suplimentare în scopul tratării cazurilor de uzurpare de identitate

(1) În cazul în care pot apărea confuzii între persoana care urmează să facă obiectul unei semnalări și o persoană a cărei identitate a fost uzurpată, sub rezerva acordului explicit al persoanei a cărei identitate a fost uzurpată, statul membru emitent adaugă în semnalare datele care o privesc pe aceasta din urmă, pentru a se evita consecințele negative ale identificării eronate. Orice persoană a cărei identitate a fost uzurpată are dreptul de a-și retrage consimțământul pentru prelucrarea datelor cu caracter personal adăugate.

(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 urmează să facă obiectul semnalării; și

(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 și sub rezerva consimțământului explicit al persoanei a cărei identitate a fost uzurpată, pentru fiecare categorie de date, se pot introduce și prelucra ulterior în SIS doar următoarele date cu caracter personal ale persoanei a cărei identitate a fost uzurpată:

(a) numele de familie;

(b) prenumele;

(c) numele la naștere;

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

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

(f) locul nașterii;

(g) data nașterii;

(h) genul;

(i) fotografii și imagini faciale;

(j) amprente digitale, amprente palmare sau ambele;

(k) orice cetățenii deținute;

(l) categoria documentelor de identificare ale persoanei;

(m) țara care a eliberat documentele de identificare ale persoanei;

(n) numărul (numerele) documentelor de identificare ale persoanei;

(o) data eliberării documentelor de identificare ale persoanei;

(p) adresa persoanei;

(q) numele tatălui persoanei;

(r) numele mamei persoanei.

(4) Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea normelor tehnice necesare privind introducerea și prelucrarea ulterioară a datelor menționate la alineatul (3) din prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

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

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

Articolul 63

Legături între semnalări

(1) Un stat membru poate crea o legătură între semnalările pe care le introduce în SIS. Scopul unei astfel de legături este de a stabili o relație între două sau mai multe semnalări.

(2) Crearea unei legături nu afectează acțiunea de urmat specifică pe baza fiecărei semnalări puse în legătură sau perioada de reexaminare a fiecăreia dintre semnalările puse în legătură.

(3) Crearea unei legături 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 legătura cu o semnalare la care nu au acces.

(4) Un stat membru creează o legătură între semnalări 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 legături între semnalări este incompatibilă cu dreptul său intern sau cu obligațiile sale internaționale, acesta poate lua măsurile necesare pentru a se asigura că respectiva legătură nu poate fi accesată de pe teritoriul său național sau de către autoritățile sale situate în afara teritoriului său.

(6) Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea normelor tehnice privind crearea unei legături între semnalări. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

Articolul 64

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 în care au fost furnizate. În orice caz, acestea se șterg 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 introdus-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 intern.

Articolul 65

Transferul datelor cu caracter personal către terți

Datele procesate în SIS și informațiile suplimentare conexe care fac obiectul schimbului în temeiul prezentului regulament nu se transferă și nu se pun la dispoziția țărilor terțe sau a organizațiilor internaționale.

CAPITOLUL XVI
Protecția datelor

Articolul 66

Legislația aplicabilă

(1) Regulamentul (UE) 2018/1725 se aplică prelucrării datelor cu caracter personal de către eu-LISA, de către Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă și de către Eurojust în temeiul prezentului regulament. Regulamentul (UE) 2016/794 se aplică prelucrării datelor cu caracter personal de către Europol în temeiul prezentului regulament.

(2) Directiva (UE) 2016/680 se aplică prelucrării datelor cu caracter personal în temeiul prezentului regulament de către autoritățile și serviciile naționale competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv în scopul protejării împotriva amenințărilor la adresa siguranței publice și al preîntâmpinării acestora.

(3) Regulamentul (UE) 2016/679 se aplică prelucrării datelor cu caracter personal în temeiul prezentului regulament de către autoritățile și serviciile naționale competente, cu excepția prelucrării în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv în scopul protejării împotriva amenințărilor la adresa siguranței publice și al preîntâmpinării acestora.

Articolul 67

Dreptul de acces, de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal

(1) Persoanele vizate au posibilitatea de a exercita drepturile prevăzute la articolele 15, 16 și 17 din Regulamentul (UE) 2016/679 și la articolul 14 și articolul 16 alineatele (1) și (2) din Directiva (UE) 2016/680.

(2) Un stat membru altul decât statul membru emitent poate furniza persoanei vizate informații privind orice date cu caracter personal ale persoanei vizate care sunt procesate, numai dacă îi oferă mai întâi statului membru emitent posibilitatea de a-și face cunoscută poziția. Comunicarea dintre statele membre respective se realizează printr-un schimb de informații suplimentare.

(3) Un stat membru ia decizia de a nu furniza, integral sau parțial, informații persoanei vizate, în conformitate cu dreptul intern, 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 vizate în cauză, pentru:

(a) a nu obstrucționa cercetările, investigațiile sau procedurile oficiale ori judiciare;

(b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;

(c) a proteja siguranța publică;

(d) a proteja securitatea națională; sau

(e) a proteja drepturile și libertățile celorlalți.

În cazurile menționate la primul paragraf, statul membru notifică persoanei vizate, în scris și fără întârzieri nejustificate, orice refuz sau restricționare a accesului, precum și motivele refuzului sau restricționării. Astfel de informații pot fi omise atunci când furnizarea acestora ar submina oricare dintre motivele prevăzute la literele (a)-(e) din primul paragraf. Statul membru informează persoana vizată despre posibilitatea de a depune o plângere la autoritatea de supraveghere sau de a introduce o cale de atac judiciară.

Statul membru justifică motivele de fapt și de drept pe care se întemeiază decizia de a nu furniza informații persoanei vizate. Aceste informații se pun la dispoziția autorităților de supraveghere.

În astfel de cazuri, persoana vizată are posibilitatea să își exercite drepturile și prin intermediul autorităților de supraveghere competente.

(4) În urma unei cereri de acces, de rectificare sau de ștergere, statul membru informează persoana vizată cât de curând posibil și, în orice caz, în termenele menționate la articolul 12 alineatul (3) din Regulamentul (UE) 2016/679 despre măsurile prin care s-a dat curs exercitării drepturilor în temeiul prezentului articol.

Articolul 68

Căi de atac

(1) Fără a aduce atingere dispozițiilor privind căile de atac din Regulamentul (UE) 2016/79 și din Directiva (UE) 2016/680, orice persoană poate introduce o acțiune în fața oricărei autorități competente, inclusiv a unei instanțe judecătorești, în temeiul dreptului oricărui stat membru, pentru accesul, rectificarea, ștergerea, obținerea informațiilor ori pentru obținerea de despăgubiri 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) din prezentul articol, fără a aduce atingere articolului 72.

(3) Statele membre prezintă anual rapoarte către Comitetul european pentru protecția datelor cu privire la:

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

(b) numărul de cereri de acces înaintate autorității 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 ștergerea datelor stocate în mod ilegal înaintate operatorului 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 de supraveghere;

(e) numărul de proceduri judiciare inițiate;

(f) numărul de cauze în care instanța judecătorească s-a pronunțat în favoarea reclamantului;

(g) orice observație privind cazurile de recunoaștere reciprocă a hotărârilor definitive pronunțate de instanțele judecătorești sau de autoritățile altor state membre privind semnalările introduse de statul membru emitent.

Comisia elaborează un model pentru rapoartele menționate la prezentul alineat.

(4) Rapoartele primite de la statele membre sunt incluse în raportul comun menționat la articolul 71 alineatul (4).

Articolul 69

Supravegherea N.SIS

(1) Statele membre se asigură că autoritățile independente de supraveghere desemnate în fiecare stat membru și învestite cu competențele menționate în capitolul VI din Regulamentul (UE) 2016/679 sau în capitolul VI din Directiva (UE) 2016/680 monitorizează legalitatea prelucrării datelor cu caracter personal din SIS pe teritoriul lor, a transmiterii acestor date de pe teritoriul lor, precum și a schimbului de informații suplimentare și a prelucrării ulterioare a acestora pe teritoriul lor.

(2) Autoritățile de supraveghere se asigură că, cel puțin din patru în patru ani, se efectuează un audit al operațiunilor de prelucrare a datelor în N.SIS, în conformitate cu standardele internaționale de audit. Auditul fie se efectuează de autoritățile de supraveghere, fie autoritățile de supraveghere dispun în mod direct efectuarea auditului de un auditor independent în materie de protecție a datelor. Autoritățile de supraveghere păstrează în permanență controlul asupra auditorului independent și își asumă responsabilitățile acestuia.

(3) Statele membre se asigură că autoritățile lor de supraveghere dispun de resurse suficiente pentru a îndeplini sarcinile care le-au fost încredințate în temeiul prezentului regulament și au acces la consiliere din partea unor persoane cu suficiente cunoștințe în domeniul datelor biometrice.

Articolul 70

Supravegherea eu-LISA

(1) Autoritatea Europeană pentru Protecția Datelor este responsabilă de monitorizarea prelucrării datelor cu caracter personal de către eu-LISA și de asigurarea faptului că aceasta se efectuează în conformitate cu prezentul regulament. Atribuțiile și competențele menționate la articolele 57 și 58 din Regulamentul (UE) 2018/1725 se aplică în consecință.

(2) Autoritatea Europeană pentru Protecția Datelor efectuează, cel puțin din patru în patru ani, un audit al prelucrării datelor cu caracter personal de către eu-LISA, în conformitate cu standardele internaționale de audit. Raportul de audit se trimite Parlamentului European, Consiliului, eu-LISA, Comisiei și autorităților de supraveghere. eu-LISA i se oferă posibilitatea de a face observații înainte de adoptarea raportului.

Articolul 71

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) Autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor, 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 de 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 prevăzute la alineatul (2), autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor se reunesc de cel puțin două ori pe an în cadrul Comitetului european pentru protecția datelor. Costurile aferente reuniunilor și organizarea acestora sunt în sarcina Comitetului european pentru protecția datelor. Cu ocazia primei reuniuni se adoptă regulamentul de procedură. Dacă este necesar, se elaborează în comun metode de lucru suplimentare.

(4) Comitetul european pentru protecția datelor transmite anual Parlamentului European, Consiliului și Comisiei un raport comun privind activitățile de supraveghere coordonată.

CAPITOLUL XVII

Răspunderea și sancțiunile

Articolul 72

Răspunderea

(1) Fără a se aduce atingere dreptului la despăgubiri și răspunderii în temeiul Regulamentului (UE) 2016/679, al Directivei (UE) 2016/680 și al Regulamentului (UE) 2018/1725:

(a) orice persoană sau stat membru care a suferit prejudicii materiale sau morale, ca urmare a unei operațiuni ilegale de prelucrare a datelor cu caracter personal prin intermediul N.SIS sau a oricărei alte acțiuni incompatibile cu prezentul regulament realizate de către un stat membru are dreptul de a primi despăgubiri din partea statului membru respectiv; și

(b) orice persoană sau stat membru care a suferit prejudicii materiale sau morale ca urmare a unei acțiuni întreprinse de către eu-LISA, incompatibile cu prezentul regulament, are dreptul de a primi despăgubiri din partea eu-LISA.

Un stat membru sau eu-LISA este exonerat(ă) de răspundere, în temeiul primului paragraf, integral sau parțial, dacă dovedește că nu este responsabil(ă) de fapta care a provocat prejudiciul.

(2) În cazul în care nerespectarea de către un stat membru a obligațiilor care îi revin în temeiul prezentului regulament produce prejudicii pentru SIS, statul membru respectiv este răspunzător pentru aceste prejudicii, cu excepția cazului și în măsura în care eu-LISA sau un alt stat membru participant la SIS nu a luat măsurile rezonabile necesare pentru a preveni producerea prejudiciilor sau pentru a diminua impactul acestora.

(3) Acțiunile în despăgubiri împotriva unui stat membru pentru prejudiciile menționate la alineatele (1) și (2) sunt reglementate de dreptul intern al statului membru respectiv. Acțiunile în despăgubiri împotriva eu-LISA pentru prejudiciile menționate la alineatele (1) și (2) sunt supuse condițiilor prevăzute în tratate.

Articolul 73

Sancțiuni

Statele membre se asigură că orice utilizare abuzivă a datelor din SIS, orice prelucrare a datelor respective sau orice schimb de informații suplimentare care contravine prezentului regulament se pedepsește în conformitate cu dreptul intern.

Sancțiunile prevăzute trebuie să fie eficace, proporționale și disuasive.

CAPITOLUL XVIII
Dispoziții finale

Articolul 74

Monitorizare și statistici

(1) eu-LISA 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 raportării, al elaborării de rapoarte privind calitatea datelor și al întocmirii de statistici, eu-LISA are acces la informațiile necesare referitoare la operațiunile de prelucrare efectuate în SIS central.

(3) eu-LISA întocmește zilnic, lunar și anual statistici care prezintă numărul de înregistrări pentru fiecare categorie de semnalări, atât pentru fiecare stat membru, cât și cumulat. De asemenea, eu-LISA furnizează rapoarte anuale privind numărul 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, atât pentru fiecare stat membru, cât și cumulat. Statisticile întocmite nu conțin date cu caracter personal. Raportul statistic anual se publică.

(4) Statele membre, Europol, Eurojust și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă furnizează eu-LISA și Comisiei informațiile necesare pentru elaborarea rapoartelor menționate la alineatele (3), (6), (8) și (9).

(5) 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, și aeronave, inclusiv motoare de aeronave, și arme de foc, sau

în numele respectivelor servicii. Statisticile arată, de asemenea, numărul de rezultate pozitive pentru fiecare categorie de semnalări.

(6) eu-LISA furnizează Parlamentului European, Consiliului, statelor membre, Comisiei, Europol, Eurojust, Agenției Europene pentru Poliția de Frontieră și Garda de Coastă, precum și Autorității Europene pentru Protecția Datelor toate rapoartele statistice pe care le elaborează.

Pentru a monitoriza punerea în aplicare a actelor juridice ale Uniunii, inclusiv în sensul Regulamentului (UE) nr. 1053/2013, Comisia poate solicita eu-LISA să furnizeze rapoarte statistice specifice suplimentare, fie periodic fie ad-hoc, privind performanța SIS, utilizarea SIS și privind schimbul de informații suplimentare.

Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă poate solicita eu-LISA să furnizeze rapoarte statistice specifice suplimentare, fie periodic, fie ad-hoc, în scopul efectuării de analize de risc și de evaluări ale vulnerabilității, astfel cum sunt menționate la articolele 11 și 13 din Regulamentul (UE) 2016/1624.

(7) În scopul articolului 15 alineatul (4) și al alineatelor (3), (4) și (6) din prezentul articol, eu-LISA instituie, pune în aplicare și găzduiește în sediile sale tehnice un registru central care conține datele menționate la articolul 15 alineatul (4) și la alineatul (3) din prezentul articol, care nu face posibilă identificarea persoanelor și care permite Comisiei și agențiilor menționate la alineatul (6) din prezentul articol să obțină rapoarte și statistici specifice. La cerere, eu-LISA acordă statelor membre și Comisiei, precum și Europol, Eurojust și Agenției Europene pentru Poliția de Frontieră și Garda de Coastă, în măsura necesară pentru îndeplinirea sarcinilor ce le revin, un acces securizat la registrul central prin intermediul infrastructurii de comunicații. eu-LISA pune în aplicare controlul accesului și profiluri de utilizator specifice, pentru a se asigura că registrul central este accesat exclusiv în scopul întocmirii de rapoarte și statistici.

(8) La doi ani de la data aplicării prezentului regulament în temeiul articolului 79 alineatul (5) primul paragraf și ulterior din doi în doi ani, eu-LISA prezintă Parlamentului European și Consiliului un raport privind funcționarea tehnică a SIS central și a infrastructurii de comunicații, inclusiv sub aspectul securității acestora, precum și privind AFIS și schimbul bilateral și multilateral de informații suplimentare dintre statele membre. Acest raport conține de asemenea, odată ce tehnologia este adoptată, o evaluare a utilizării imaginilor faciale pentru identificarea persoanelor.

(9) La trei ani de la data aplicării prezentului regulament în temeiul articolului 79 alineatul (5) primul paragraf și ulterior o dată la patru ani, Comisia efectuează o evaluare globală a SIS central și a schimburilor bilaterale și multilaterale de informații suplimentare între 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. Raportul de evaluare include de asemenea o evaluare a AFIS și a campaniilor de informare privind SIS desfășurate de Comisie în conformitate cu articolul 19.

Comisia transmite raportul de evaluare Parlamentului European și Consiliului.

(10) Comisia adoptă acte de punere în aplicare pentru stabilirea unor norme detaliate privind funcționarea registrului central menționat la alineatul (7) din prezentul articol și privind normele de protecție a datelor și normele de securitate aplicabile respectivului registru. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 76 alineatul (2).

Articolul 75

Exercitarea delegării de competențe

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

(2) Competența de a adopta acte delegate menționată la articolul 38 alienatul (3) și la articolul 43 alineatul (4) se conferă Comisiei pe o perioadă nedeterminată de la 27 decembrie 2018.

(3) Delegarea de competențe menționată la articolul 38 alineatul (3) și la articolul 43 alineatul (4) poate fi revocată în orice moment de către Parlamentul European sau de către Consiliu. O decizie de revocare pune

capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în Jurnalul Oficial al Uniunii Europene sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

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

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

(6) Un act delegat adoptat în temeiul articolului 38 alineatul (3) sau al articolului 43 alineatul (4) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecțiuni în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecțiuni. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 76

Procedura comitetului

(1) Comisia este asistată de un comitet. Comitetul respectiv este un comitet în înțelesul 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 77

Modificarea Deciziei 2007/533/JAI

Decizia 2007/533/JAI se modifică după cum urmează:

1.Articolul 6 se înlocuiește cu următorul text:

„Articolul 6

Sistemele naționale

(1) Fiecare stat membru este responsabil cu înființarea, funcționarea, întreținerea și dezvoltarea în continuare a N.SIS II propriu și cu conectarea acestuia la NI-SIS.

(2) Fiecare stat membru este responsabil cu asigurarea disponibilității neîntrerupte a datelor din SIS II pentru utilizatorii finali.”

2.Articolul 11 se înlocuiește cu următorul text:

„Articolul 11

Confidențialitatea – Statele membre

(1) Fiecare stat membru aplică propriile norme în domeniul secretului profesional sau alte obligații echivalente de confidențialitate pentru toate persoanele și organismele care lucrează cu date din SIS II și alte informații suplimentare, în conformitate cu legislația națională. Această obligație se aplică și după ce persoanele respective au încetat să mai ocupe o anumită funcție sau un anumit post ori după încetarea activităților organismelor respective.

(2) Dacă un stat membru colaborează cu contractanți externi în cadrul oricăror sarcini legate de SIS II, acesta monitorizează îndeaproape activitățile contractanților pentru a asigura respectarea tuturor dispozițiilor prezentei decizii, în special a celor referitoare la securitate, la confidențialitate și la protecția datelor.

(3) Gestionarea operațională a N.SIS II sau a copiilor tehnice nu se încredințează societăților private și nici organizațiilor private.”

3.Articolul 15 se modifică după cum urmează:

(a)se introduce următorul alineat:

„(3a) Autoritatea de gestionare dezvoltă și menține un mecanism și proceduri pentru verificarea calității datelor în CS-

SIS. Autoritatea de gestionare prezintă rapoarte periodice statelor membre în acest sens.

Autoritatea de gestionare prezintă Comisiei un raport periodic care se referă la problemele întâmpinate și la statele membre vizate.

Comisia prezintă Parlamentului European și Consiliului un raport periodic cu privire la problemele întâmpinate legate de calitatea datelor.”;

(b)alineatul (8) se înlocuiește cu următorul text:

„(8) Gestionarea operațională a SIS II central constă în toate sarcinile necesare menținerii SIS II central în funcțiune 24 de ore pe zi, șapte zile pe săptămână în conformitate cu prezenta decizie, în special în activitatea de întreținere și în evoluția tehnică necesare pentru buna funcționare a sistemului. Aceste sarcini trebuie să includă, de asemenea, coordonarea, gestionarea și sprijinirea activităților de testare pentru SIS II central și N.SIS II, care să asigure că SIS II central și N.SIS II funcționează în conformitate cu cerințele pentru conformitatea tehnică stabilite la articolul 9.”

4.La articolul 17 se adaugă următoarele alineate:

„(3) Dacă autoritatea de gestionare colaborează cu contractanți externi în cadrul oricăror sarcini legate de SIS II, aceasta monitorizează îndeaproape activitățile contractanților pentru a asigura respectarea tuturor dispozițiilor prezentei decizii, în special referitoare la securitate, la confidențialitate și la protecția datelor.

(4) Gestionarea operațională a CS-SIS nu se încredințează societăților private și nici organizațiilor private.”

5.La articolul 21 se adaugă următorul paragraf:

„În cazul în care se caută o persoană sau un obiect în temeiul unei semnalări legate de o infracțiune de terorism, cazul este considerat suficient de adecvat, relevant și important pentru a justifica o semnalare în SIS II. Din motive de siguranță publică sau de securitate națională, statele membre pot, în mod excepțional, să nu introducă o semnalare atunci când aceasta este de natură să obstrucționeze cercetările, investigațiile sau procedurile oficiale ori judiciare.”

6.Articolul 22 se înlocuiește cu următorul text:

„Articolul 22

Norme specifice privind introducerea, verificarea sau efectuarea de căutări prin utilizarea fotografiilor și a amprentelor digitale

(1) Fotografiile și amprentele digitale se introduc doar în urma unei verificări speciale a calității, care să garanteze faptul că respectă standardele minime de calitate a datelor. Specificațiile pentru verificările speciale de calitate se stabilesc în conformitate cu procedura menționată la articolul 67.

(2) În cazul în care o semnalare din SIS II conține fotografii și date dactiloscopice, respectivele fotografii și date dactiloscopice se utilizează pentru a confirma identitatea unei persoane care a fost localizată în urma unei căutări alfanumerice efectuate în SIS II.

(3) Se pot efectua căutări în datele dactiloscopice în orice situație în scopul identificării unei persoane. Cu toate acestea, se efectuează căutări în datele dactiloscopice în scopul identificării în cazul în care identitatea unei persoane nu poate fi stabilită prin niciun alt mijloc. În acest scop, sistemul SIS II central conține un sistem automat de identificare a amprentelor digitale (AFIS).

(4) Se pot efectua căutări în datele dactiloscopice din SIS II în legătură cu semnalări introduse în conformitate cu articolele 26, 32 și 36 și prin utilizarea unor seturi complete sau incomplete de amprente digitale descoperite la locul comiterii unor infracțiuni grave sau al unor infracțiuni de terorism în curs de investigare, în cazul în care se poate stabili cu un grad ridicat de probabilitate că respectivele seturi de amprente aparțin unui autor al infracțiunii și cu condiția să se efectueze simultan o căutare în bazele de date dactiloscopice naționale relevante ale statului membru.”

7.Articolul 41 se înlocuiește cu următorul text:

„Articolul 41

Accesul la date în SIS II de către Europol

(1) Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol), instituită prin Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului (*1) are dreptul de acces la date în SIS II și de a efectua căutări în acestea, în cazurile în care acest lucru este necesar pentru îndeplinirea mandatului său. De asemenea, Europol poate face schimb de informații suplimentare și poate solicita informații suplimentare în conformitate cu dispozițiile din manualul SIRENE.

(2) Atunci când o căutare efectuată de Europol indică existența unei semnalări în SIS II, Europol informează statul membru emitent, printr-un schimb de informații suplimentare, cu ajutorul infrastructurii de comunicații și în conformitate cu dispozițiile prevăzute de manualul SIRENE. Până când Europol va putea utiliza funcționalitățile prevăzute în vederea schimbului de informații suplimentare, acesta informează statul membru emitent prin intermediul canalelor definite de Regulamentul (UE) 2016/794.

(3) Europol poate prelucra informațiile suplimentare pe care i le-au furnizat statele membre pentru a efectua comparații cu bazele sale de date și cu proiectele sale de analiză operațională, în scopul identificării conexiunilor sau a altor legături relevante, precum și pentru analizele strategice, tematice și operaționale, menționate la articolul 18 alineatul (2) literele (a), (b) și (c) din Regulamentul (UE) 2016/794. Orice prelucrare de către Europol a informațiilor suplimentare în scopul prezentului articol se efectuează în conformitate cu respectivul regulament.

(4) Utilizarea de către Europol a informațiilor obținute în urma efectuării unei căutări în SIS II sau a prelucrării de informații suplimentare este condiționată de acordul statului membru emitent. Dacă statul membru permite utilizarea informațiilor respective, tratarea acestora de către Europol intră sub incidența Regulamentului (UE) 2016/794. Europol comunică astfel de informații țărilor terțe și organismelor terțe numai cu acordul statului membru emitent și în cu respectarea deplină a dreptului Uniunii în materie de protecție a datelor.

(5) Europol:

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

(b) în pofida articolului 31 alineatul (1) din Regulamentul (UE) 2016/794, șterge informațiile suplimentare care conțin date cu caracter personal cel târziu la un an de la ștergerea semnalării conexe. Prin derogare, în situațiile în care Europol deține, în bazele sale de date sau în cadrul proiectelor sale de analiză operațională, informații cu privire la un caz cu care informațiile suplimentare au legătură, Europol poate, în mod excepțional, pentru a-și putea îndeplini sarcinile, să continue să stocheze informațiile suplimentare atunci când este necesar. Europol informează statul membru emitent și statul membru de executare despre menținerea stocării unor astfel de informații suplimentare și prezintă o motivare în acest sens;

(c) limitează accesul la date în SIS II, inclusiv la informațiile suplimentare, la personalul său autorizat în mod expres în acest sens care are nevoie de acces la astfel de date pentru îndeplinirea sarcinilor care îi revin;

(d) adoptă și aplică măsuri menite să asigure securitatea, confidențialitatea și automonitorizarea în conformitate cu articolele 10, 11 și 13;

(e) se asigură că personalul său care este autorizat să prelucreze datele din SIS II beneficiază de o formare profesională și de o informare adecvate, în conformitate cu articolul 14; și

(f) fără a aduce atingere Regulamentului (UE) 2016/794, permite Autorității Europene pentru Protecția Datelor să monitorizeze și să examineze activitățile pe care le desfășoară Europol în exercitarea dreptului său de acces la date în SIS II și de a efectua căutări în acestea, precum și în ceea ce privește schimbul de informații suplimentare și prelucrarea acestora.

(6) Europol copiază date din SIS II numai în scopuri tehnice, atunci când respectiva copiere să fie necesară pentru ca personalul Europol autorizat în mod corespunzător să efectueze o căutare directă. Prezenta decizie se aplică copiilor respective. Copia tehnică se utilizează numai pentru stocarea datelor din SIS II în timp ce se efectuează căutări în aceste date. După ce s-au efectuat căutări în date, acestea se șterg. Aceste utilizări nu se consideră a constitui o descărcare sau o copiere ilegală a datelor din SIS II. Europol nu copiază în alte sisteme ale sale datele semnalărilor sau datele suplimentare emise de statele membre ori datele din CS-SIS II.

(7) În scopul verificării legalității prelucrării datelor, al automonitorizării și al asigurării securității și integrității corespunzătoare a datelor, Europol păstrează înregistrările fiecărei accesări a SIS II și fiecărei căutări în SIS II în conformitate cu dispozițiile articolului 12. Astfel de înregistrări și documentații nu se consideră a constitui o descărcare sau o copiere ilegală a vreunei părți din SIS II.

(8) Statele membre informează Europol, printr-un schimb de informații suplimentare, ori de câte ori obțin un rezultat pozitiv legat de semnalări referitoare la infracțiuni de terorism. În mod excepțional, statele membre pot să nu informeze Europol în cazul în care informarea acestuia ar pune în pericol investigații în curs sau siguranța unei persoane ori ar fi contrară intereselor esențiale legate de securitatea statului membru emitent.

(9) Alineatul (8) se aplică începând cu data la care Europol este în măsură să primească informații suplimentare în conformitate cu alineatul (1).

(*1) Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului (JO L 135, 24.5.2016, p. 53).”"

8. Se introduce următorul articol:

„Articolul 42a

Accesul la date în SIS de către echipele europene de poliție de frontieră și gardă de coastă, echipele formate din personalul implicat în sarcini legate de returnare și membrii echipelor de sprijin pentru gestionarea migrației

(1) În conformitate cu articolul 40 alineatul (8) din Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului (*2), membrii echipelor menționate la articolul 2 punctele 8 și 9 din regulamentul respectiv, în conformitate cu mandatele lor respective și

cu condiția să fie autorizați să efectueze controale în conformitate cu articolul 40 alineatul (1) din prezenta decizie și să fi beneficiat de formarea necesară în conformitate cu articolul 14 din prezenta decizie, au dreptul de acces la date în SIS II și de a efectua căutări în acestea, în măsura în care este necesar pentru îndeplinirea sarcinilor ce le revin și în măsura impusă de planul operațional pentru o operațiune specifică. Accesul la date în SIS II nu se acordă membrilor altor echipe.

(2) Membrii echipelor menționate la alineatul (1) își exercită dreptul de acces la date în SIS II și de a efectua căutări în acestea în conformitate cu alineatul (1) prin intermediul unei interfețe tehnice. Interfața tehnică este creată și întreținută de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă și permite conectarea directă la SIS II central.

(3) Atunci când o căutare efectuată de un membru al echipelor menționate la alineatul (1) din prezentul articol indică existența unei semnalări în SIS II, statul membru emitent este informat cu privire la aceasta. În conformitate cu articolul 40 din Regulamentul (UE) 2016/1624, membrii echipelor acționează ca răspuns la o semnalare în SIS II numai dacă primesc instrucțiuni de la polițiștii de frontieră sau de la membrii personalului implicați în sarcini legate de returnare ai statului membru gazdă în care își desfășoară activitatea și, ca regulă generală, în prezența acestora. Statul membru gazdă poate autoriza membrii echipelor să acționeze în numele său.

(4) În scopul verificării legalității prelucrării datelor, al automonitorizării și al asigurării securității și integrității corespunzătoare a datelor, Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă păstrează înregistrările fiecărei accesări a SIS II și fiecărei căutări în SIS II în conformitate cu dispozițiile articolului 12.

(5) Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă adoptă și aplică măsuri menite să asigure securitatea, confidențialitatea și automonitorizarea în conformitate cu articolele 10, 11 și 13 și se asigură că echipele menționate la alineatul (1) din prezentul articol aplică aceste măsuri.

(6) Nicio dispoziție a prezentului articol nu se interpretează ca aducând atingere dispozițiilor Regulamentului (UE) 2016/1624 în ceea ce privește protecția datelor sau și răspunderii Agenției Europene pentru Poliția de Frontieră și Garda de Coastă pentru orice prelucrare neautorizată sau incorectă a datelor de către aceasta.

(7) Fără a aduce atingere alineatului (2), nicio parte a SIS II nu se conectează la niciun sistem pentru colectarea și prelucrarea datelor operat de echipele menționate la alineatul (1) sau de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă, iar datele din SIS II la care aceste echipe au acces nu se transferă către un astfel de sistem. Nicio parte a SIS II nu se descarcă și nu se copiază. Înregistrarea accesului și a căutărilor nu se consideră a constitui o descărcare sau o copiere ilegală a datelor din SIS II.
(8) Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă permite Autorității Europene pentru Protecția Datelor să monitorizeze și să examineze activitățile echipelor menționate la prezentul articol în contextul exercitării de către acestea a dreptului de acces la date în SIS II și de a efectua căutări în acestea. Acest lucru nu aduce atingere altor dispoziții din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului (*3).
(*2) 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)."
(*3) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).'"

Articolul 78

Abrogare

Regulamentul (CE) nr. 1986/2006 și Deciziile 2007/533/JAI și 2010/261/UE se abrogă de la data aplicării prezentului regulament astfel cum este prevăzută la articolul 79 alineatul (5) primul paragraf.

Trimiterile la Regulamentul (CE) nr. 1986/2006 abrogat și la Decizia 2007/533/JHA abrogată se interpretează ca trimiteri la prezentul regulament și se citesc în conformitate cu tabelele de corespondență din anexă.

Articolul 79

Intrarea în vigoare, intrarea în funcțiune și aplicarea

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

(2) Cel târziu la 28 decembrie 2021, Comisia adoptă o decizie prin care stabilește data la care operațiunile SIS debutează în temeiul prezentului regulament, după ce verifică dacă au fost îndeplinite următoarele condiții:

(a) au fost adoptate actele de punere în aplicare necesare pentru aplicarea prezentului regulament;

(b)statele membre au notificat Comisiei că au luat măsurile tehnice și juridice necesare pentru prelucrarea datelor din SIS și pentru

efectuarea schimbului de informații suplimentare în temeiul prezentului regulament; și

(c) eu-LISA a notificat Comisiei finalizarea cu succes a tuturor activităților de testare în ceea ce privește CS-SIS și interacțiunea dintre CS.SIS și N-SIS.

(3) Comisia monitorizează îndeaproape desfășurarea procesului care conduce la îndeplinirea treptată a condițiilor prevăzute la alineatul (2) și informează Parlamentul European și Consiliul în legătură cu rezultatul verificărilor menționate la alineatul respectiv.

(4) Până la 28 decembrie 2019 și ulterior în fiecare an până la adoptarea deciziei Comisiei menționate la alineatul (2), Comisia prezintă un raport Parlamentului European și Consiliului privind stadiul pregătirilor pentru punerea deplină în aplicare a prezentului regulament. Acest raport conține totodată informații detaliate cu privire la costurile aferente și la orice risc care poate avea un impact asupra costurilor totale.

(5) Prezentul regulament se aplică de la data stabilită în conformitate cu alineatul (2).

Prin derogare de la primul paragraf:

(a) articolul 4 alineatul (4), articolul 5, articolul 8 alineatul (4), articolul 9 alineatele (1) și (5), articolul 12 alineatul (8), articolul 15 alineatul (7), articolul 19, articolul 20 alineatele (4) și (5), articolul 26 alineatul (6), articolul 32 alineatul (9), articolul 34 alineatul (3), articolul 36 alineatul (6), articolul 38 alineatele (3) și (4), articolul 42 alineatul (5), articolul 43 alineatul (4), articolul 54 alineatul (5), articolul 62 alineatul (4), articolul 63 alineatul (6), articolul 74 alineatele (7) și (10), articolul 75, articolul 76, articolul 77 punctele 1-5, precum și alineatele (3) și (4) din prezentul articol se aplică de la data intrării în vigoare a prezentului regulament;

(b) articolul 77 punctele 7 și 8 se aplică de la 28 decembrie 2019;

(c) articolul 77 punctul 6 se aplică de la 28 decembrie 2020.

(6) Decizia Comisiei menționată la alineatul (2) se publică în *Jurnalul Oficial al Uniunii Europene*.

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

Adoptat la Bruxelles, 28 noiembrie 2018.

Pentru Parlamentul European
Președintele
A. TAJANI

Pentru Consiliu
Președintele
K. EDTSTADLER

([1]) Poziția Parlamentului European din 24 octombrie 2018 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 19 noiembrie 2018.

([2]) JO L 239, 22.9.2000, p. 19.

([3]) Regulamentul (CE) nr. 2424/2001 al Consiliului din 6 decembrie 2001 privind dezvoltarea Sistemului de Informații Schengen de a doua generație (SIS II) (JO L 328, 13.12.2001, p. 4).

([4]) 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).

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

([6]) 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).

([7]) Regulamentul (UE) 2018/1861 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Convenției de punere în aplicare a Acordului Schengen și de modificare și abrogare a Regulamentului (CE) nr. 1987/2006 (a se vedea pagina 14 din prezentul Jurnal Oficial).

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

([9]) 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).
([10]) 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).
([11]) 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).
([12]) 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).
([13]) 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).
([14]) Directiva 2013/48/UE a Parlamentului European și a Consiliului din 22 octombrie 2013 privind dreptul de a avea acces la un avocat în cadrul procedurilor penale și al procedurilor privind mandatul european de arestare, precum și dreptul ca o persoană terță să fie informată în urma privării de libertate și dreptul de a comunica cu persoane terțe și cu autorități consulare în timpul privării de libertate (JO L 294, 6.11.2013, p. 1).
([15]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39)
([16]) Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului (JO L 135, 24.5.2016, p. 53).
([17]) JO L 56, 4.3.1968, p. 1.
([18]) 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).
([19]) 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).
([20]) JO L 123, 12.5.2016, p. 1.
([21]) Decizia 2000/365/CE a Consiliului din 29 mai 2000 privind solicitarea Regatului Unit al Marii Britanii și Irlandei de Nord de a participa la unele dintre dispozițiile acquis-ului Schengen (JO L 131, 1.6.2000, p. 43).
([22]) Decizia 2002/192/CE a Consiliului din 28 februarie 2002 privind solicitarea Irlandei de a participa la unele dintre dispozițiile acquis-ului Schengen (JO L 64, 7.3.2002, p. 20).
([23]) JO L 176, 10.7.1999, p. 36.
([24]) Decizia 1999/437/CE a Consiliului din 17 mai 1999 privind anumite modalități de aplicare a Acordului încheiat între Consiliul Uniunii Europene și Republica Islanda și Regatul Norvegiei în ceea ce privește asocierea acestor două state în vederea punerii în aplicare, a asigurării respectării și dezvoltării acquis-ului Schengen (JO L 176, 10.7.1999, p. 31).
([25]) JO L 53, 27.2.2008, p. 52.
([26]) Decizia 2008/149/JAI a Consiliului din 28 ianuarie 2008 privind încheierea, în numele Uniunii Europene, a Acordului între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană cu privire la asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen (JO L 53, 27.2.2008, p. 50).
([27]) JO L 160, 18.6.2011, p. 21.
([28]) 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).
([29]) Decizia 2010/365/UE a Consiliului din 29 iunie 2010 privind aplicarea dispozițiilor acquis-ului Schengen referitoare la Sistemul de informații Schengen în Republica Bulgaria și în România (JO L 166, 1.7.2010, p. 17).
([30]) Decizia (UE) 2018/934 a Consiliului din 25 iunie 2018 privind punerea în aplicare a dispozițiilor rămase ale acquis-ului Schengen referitoare la Sistemul de informații Schengen în Republica Bulgaria și în România (JO L 165, 2.7.2018, p. 37).
([31]) Decizia (UE) 2017/733 a Consiliului din 25 aprilie 2017 privind aplicarea dispozițiilor acquis-ului Schengen referitoare la Sistemul de informații Schengen în Republica Croația (JO L 108, 26.4.2017, p. 31).
([32]) 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).
([33]) 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).
([34]) 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).

([35]) Directiva (UE) 2017/541 a Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului (JO L 88, 31.3.2017, p. 6).
([36]) Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului din 9 martie 2016 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen) (JO L 77, 23.3.2016, p. 1).
([37]) Regulamentul (UE) nr. 1053/2013 al Consiliului 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).
([38]) Directiva 2013/32/UE a Parlamentului European și a Consiliului din 26 iunie 2013 privind procedurile comune de acordare și retragere a protecției internaționale (JO L 180, 29.6.2013, p. 60).
([39]) Regulamentul (CE) nr. 377/2004 al Consiliului din 19 februarie 2004 privind crearea unei rețele de ofițeri de legătură în materie de imigrație (JO L 64, 2.3.2004, p. 1).
([40]) Directiva 1999/37/CE a Consiliului din 29 aprilie 1999 privind documentele de înmatriculare pentru vehicule (JO L 138, 1.6.1999, p. 57).
([41]) Regulamentul (UE) 2018/1727 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust) și de înlocuire și abrogare a Deciziei 2002/187/JAI a Consiliului (JO L 295, 21.11.2018, p. 138).

ANEXĂ

TABEL DE CORESPONDENȚĂ

Decizia 2007/533/JHA	**Prezentul regulament**
Articolul 1	Articolul 1
Articolul 2	Articolul 2
Articolul 3	Articolul 3
Articolul 4	Articolul 4
Articolul 5	Articolul 5
Articolul 6	Articolul 6
Articolul 7	Articolul 7
Articolul 8	Articolul 8
Articolul 9	Articolul 9
Articolul 10	Articolul 10
Articolul 11	Articolul 11
Articolul 12	Articolul 12
Articolul 13	Articolul 13
Articolul 14	Articolul 14
Articolul 15	Articolul 15
Articolul 16	Articolul 16
Articolul 17	Articolul 17
Articolul 18	Articolul 18
Articolul 19	Articolul 19
Articolul 20	Articolul 20
Articolul 21	Articolul 21
Articolul 22	Articolele 42 și 43
Articolul 23	Articolul 22
—	Articolul 23
Articolul 24	Articolul 24

Articolul 25	Articolul 25
Articolul 26	Articolul 26
Articolul 27	Articolul 27
Articolul 28	Articolul 28
Articolul 29	Articolul 29
Articolul 30	Articolul 30
Articolul 31	Articolul 31
Articolul 32	Articolul 32
Articolul 33	Articolul 33
Articolul 34	Articolul 34
Articolul 35	Articolul 35
Articolul 36	Articolul 36
Articolul 37	Articolul 37
Articolul 38	Articolul 38
Articolul 39	Articolul 39
—	Articolul 40
—	Articolul 41
Articolul 40	Articolul 44
—	Articolul 45
—	Articolul 46
—	Articolul 47
Articolul 41	Articolul 48
Articolul 42	Articolul 49
—	Articolul 51
Articolul 42a	Articolul 50
Articolul 43	Articolul 52
Articolul 44	Articolul 53
Articolul 45	Articolul 54
—	Articolul 55
Articolul 46	Articolul 56
Articolul 47	Articolul 57
Articolul 48	Articolul 58
Articolul 49	Articolul 59
—	Articolul 60
Articolul 50	Articolul 61
Articolul 51	Articolul 62
Articolul 52	Articolul 63
Articolul 53	Articolul 64
Articolul 54	Articolul 65
Articolul 55	—

Articolul 56	—
Articolul 57	Articolul 66
Articolul 58	Articolul 67
Articolul 59	Articolul 68
Articolul 60	Articolul 69
Articolul 61	Articolul 70
Articolul 62	Articolul 71
Articolul 63	—
Articolul 64	Articolul 72
Articolul 65	Articolul 73
Articolul 66	Articolul 74
—	Articolul 75
Articolul 67	Articolul 76
Articolul 68	—
—	Articolul 77
Articolul 69	—
—	Articolul 78
Articolul 70	—
Articolul 71	Articolul 79

Regulamentul (CE) nr. 1986/2006	**Prezentul regulament**
Articolele 1, 2 şi 3	Articolul 45