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

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

hotărând în conformitate cu procedura legislativă ordinară ([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 și 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]). SIS II 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), cu articolul 43 alineatul (3) și cu 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, precum 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 capitolul 2 din Tratatul privind funcționarea Uniunii Europene (TFUE). Regulamentul (UE) 2018/1862 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 capitolele 4 și 5 din TFUE.

([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 din 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) 2018/1862 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 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 (a se vedea pagina 56 din prezentul Jurnal Oficial).

(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 și prelucrarea datelor.

(7) Semnalările din SIS conțin doar informațiile necesare pentru identificarea unei persoane 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. Statele membre ar trebui să asigure, de asemenea, o conectare 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, 7 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 ([1]) 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

([1]) 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).

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 privind presiunea migrației și gestionarea frontierelor, 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 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 în registrul respectiv sau obținute din acesta 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, semnalările pentru refuzul intrării și al șederii ar trebui să conțină informații privind decizia pe care se bazează semnalarea. În plus, pentru a facilita identificarea și a depista identitățile multiple, semnalarea ar trebui să includă, 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 date 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 evita inconvenientele cauzate de identificarea eronată, 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 ([1]) și la articolul 5 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([2]). 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.

([1]) 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).

([2]) 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).

(23) 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 acestea 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.

(24) 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.

(25) 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.

(26) Un nivel mai ridicat de eficacitate, armonizare și consecvență se poate realiza prin impunerea obligației de a introduce în SIS toate interdicțiile de intrare emise de autoritățile naționale competente în conformitate cu proceduri care respectă Directiva 2008/115/CE a Parlamentului European și a Consiliului ([1]) și prin stabilirea de norme comune pentru introducerea semnalărilor pentru refuzul intrării și al șederii în urma returnării unui resortisant al unei țări terțe aflat în situație de ședere ilegală. Statele membre ar trebui să ia toate măsurile necesare pentru a se asigura că nu există un decalaj temporar între momentul părăsirii spațiului Schengen de către resortisantul țării terțe vizat și activarea semnalării în SIS. Acest fapt ar trebui să garanteze asigurarea respectării interdicțiilor de intrare la punctele de trecere a frontierelor externe, prevenind în mod eficace reintrarea în spațiul Schengen.

(27) Persoanele în privința cărora s-a luat o decizie de refuz al intrării și al șederii ar trebui să aibă dreptul la o cale de atac împotriva deciziei respective. Dreptul la o cale de atac ar trebui să respecte Directiva 2008/115/CE atunci când decizia se referă la returnare.

(28) Prezentul regulament ar trebui să stabilească norme obligatorii privind consultarea și notificarea autorităților naționale în cazul în care un resortisant al unei țări terțe deține sau ar putea obține un permis de ședere valabil sau o viză de lungă ședere acordată într-un stat membru și un alt stat membru intenționează să emită sau a introdus deja o semnalare privind refuzul intrării și al șederii pentru respectivul resortisant al unei țări terțe. Aceste situații creează incertitudini grave pentru polițiștii de frontieră, pentru poliție și pentru autoritățile din domeniul imigrației. Prin urmare, este oportun să se prevadă un termen obligatoriu de consultare rapidă cu un rezultat precis pentru a se asigura că resortisanții țărilor terțe care au drept de ședere legală pe teritoriul statelor membre pot intra pe teritoriul respectiv fără dificultăți, iar cei care nu au drept de intrare sunt împiedicați să facă acest lucru.

(29) La ștergerea unei semnalări în SIS în urma unei consultări între statele membre, statul membru emitent ar trebui să poată menține resortisantul unei țări terțe vizat pe lista sa națională de semnalări.

(30) Prezentul regulament nu ar trebui să aducă atingere aplicării Directivei 2004/38/CE a Parlamentului European și a Consiliului ([2]).

(31) Semnalările nu ar trebui păstrate în SIS mai mult timp decât este necesar în vederea îndeplinirii scopurilor specifice în care au fost introduse. În termen de trei ani de la introducerea unei semnalări în SIS, statul membru emitent ar trebui să reexamineze nevoia de a o păstra. Cu toate acestea, dacă decizia națională pe care se bazează semnalarea prevede o perioadă de valabilitate mai lungă de trei ani, semnalarea ar trebui reexaminată în termen de cinci ani. 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 în timpul perioadei de reexaminare stabilite și ar trebui să întocmească statistici referitoare la numărul de semnalări referitoare la persoane în cazul cărora care s-a prelungit perioada de păstrare.

(32) 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 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.

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

([2]) Directiva 2004/38/CE a Parlamentului European și a Consiliului din 29 aprilie 2004 privind dreptul la liberă circulație și ședere pe teritoriul statelor membre pentru cetățenii Uniunii și membrii familiilor acestora, de modificare a Regulamentului (CEE) nr. 1612/68 și de abrogare a Directivelor 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE și 93/96/CEE (JO L 158, 30.4.2004, p. 77).

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

(34) 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.

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

(36) 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 urmăririi penale a infracțiunilor de terorism sau a altor infracțiuni grave.

(37) 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 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 sau a altor infracțiuni grave ori al executării pedepselor. Accesul la datele introduse în SIS și dreptul de a efectua căutări în astfel de 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.

(38) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([1]) 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.

(39) Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului ([2]) ar trebui să se aplice prelucrărilor de date cu caracter personal efectuate de către Europol în temeiul prezentului regulament.

(40) 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.

(41) 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 ([3]) (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.

(42) 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 să coopereze pentru a aborda aspectele legate de securitate dintr-o perspectivă comună.

(43) 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.

([1]) 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).

([2]) 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).

([3]) JO L 56, 4.3.1968, p. 1.

(44) 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 statul membru respectiv 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.

(45) 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.

(46) 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.

(47) 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. Pentru a facilita îndeplinirea de către Europol a sarcinilor care îi revin, în special în cadrul Centrului european privind traficul de migranți, este oportun să se permită accesul Europol la categoriile de semnalări prevăzute în prezentul regulament.

(48) 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.

(49) 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.

(50) Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului ([1]) 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 efectuate în SIS 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 al personalului 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.

(51) 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

([1]) 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).

priorității semnalărilor, privind legăturile dintre semnalări 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.

(52) În vederea asigurării unor condiții uniforme de punere 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 ([1]). Procedura de adoptare a actelor de punere în aplicare în temeiul prezentului regulament și al Regulamentului (UE) 2018/1862 ar trebui să fie aceeași.

(53) 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.

(54) 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 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 ([2]). 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.

(55) Întrucât obiectivele prezentului regulament, și anume instituirea și reglementarea unui sistem de informații al Uniunii și schimbul de informații suplimentare conexe, nu pot să fie realizate în mod satisfăcător de statele membre dar, având în vedere însăși 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.

(56) 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 protecția migranților aflați în situație ilegală împotriva exploatării și a traficului de ființe umane. În cazurile referitoare la copii, interesul superior al copilului ar trebui să primeze.

(57) Costurile estimate aferente actualizării sistemelor naționale și punerii în aplicare a noilor funcționalități prevăzute în prezentul regulament sunt mai mici decât suma rămasă la linia bugetară pentru frontiere inteligente din Regulamentul (UE) nr. 515/2014 al Parlamentului European și al Consiliului ([3]). Prin urmare, finanțarea atribuită dezvoltării de sisteme informatice de sprijin pentru gestionarea fluxurilor migratorii la frontierele externe în conformitate cu Regulamentul (UE) nr. 515/2014 ar trebui să fie alocată statelor membre și eu-LISA. Costurile financiare aferente actualizării SIS și punerii în aplicare a prezentului regulamentul ar trebui să fie monitorizate. În cazul în care costurile estimate sunt mai ridicate, ar trebui să se pună la dispoziție finanțare din partea Uniunii pentru a sprijini statele membre în conformitate cu cadrul financiar multianual aplicabil.

(58) 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 daca îl va pune în aplicare în legislația sa națională.

([1]) 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).

([2]) JO L 123, 12.5.2016, p. 1.

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

(59) Prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen la care Regatul Unit nu participă, în conformitate cu Decizia 2000/365/CE a Consiliului ([1]); prin urmare, Regatul Unit nu participă la adoptarea prezentului regulament, acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică.

(60) Prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen la care Irlanda nu participă, în conformitate cu Decizia 2002/192/CE a Consiliului ([2]); prin urmare, Irlanda nu participă la adoptarea prezentului regulament, acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică.

(61) 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 ([3]), care se află sub incidența articolului 1 punctul G din Decizia 1999/437/CE a Consiliului ([4]).

(62) În ceea ce privește Elveția, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Acordului dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană cu privire la asocierea Confederației Elvețiene la punerea în aplicare, asigurarea respectării și dezvoltarea acquis-ului Schengen ([5]), care se află sub incidența articolului 1 punctul G din Decizia 1999/437/CE coroborat cu articolul 3 din Decizia 2008/146/CE a Consiliului ([6]).

(63) 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 ([7]), care se află sub incidența articolului 1 punctul G din Decizia 1999/437/CE, coroborat cu articolul 3 din Decizia 2011/350/UE a Consiliului ([8]).

(64) În ceea ce privește Bulgaria și România, prezentul regulament constituie un act care se întemeiază pe acquis-ul Schengen sau 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 ([9]) și (UE) 2018/934 ([10]) ale Consiliului.

(65) În ceea ce privește Croația, prezentul regulament constituie un act care se întemeiază pe acquis-ul Schengen sau 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 ([11]).

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

(67) 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

---

([1]) 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).

([2]) 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).

([3]) JO L 176, 10.7.1999, p. 36.

([4]) 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).

([5]) JO L 53, 27.2.2008, p. 52.

([6]) Decizia 2008/146/CE a Consiliului din 28 ianuarie 2008 privind încheierea, în numele Comunității 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. 1).

([7]) JO L 160, 18.6.2011, p. 21.

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

([9]) 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).

([10]) 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).

([11]) 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).

introduce modificări ale Regulamentului (CE) nr. 1987/2006 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.

(68) Regulamentul (CE) nr. 1987/2006 ar trebui abrogat de la data aplicării integrale a prezentului regulament.

(69) 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 ([1]) 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 2 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 privind resortisanții țărilor terțe, precum și la schimbul de informații suplimentare și de date suplimentare în scopul refuzului intrării și al șederii pe teritoriul statelor membre.

(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 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;

([1]) 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).

4. „resortisant al unei țări terțe” înseamnă orice persoană care nu este cetățean al Uniunii în înțelesul articolului 20 alineatul (1) din TFUE, cu excepția persoanelor care beneficiază de drepturi de liberă circulație echivalente cu cele ale cetățenilor Uniunii în temeiul acordurilor dintre Uniune sau dintre Uniune și statele sale membre, pe de o parte, și țări terțe, pe de altă parte;

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

6. „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;

7. „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;

8. „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;

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

10. „stat membru de acordare” înseamnă statul membru care ia în considerare acordarea sau prelungirea sau care a acordat sau a prelungit un permis de ședere sau o viză de lungă ședere și care este implicat în procedura de consultare cu alt stat membru;

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

12. „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;

13. „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 și date dactiloscopice;

14. „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;

15. „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;

16. „returnare” înseamnă returnare astfel cum este definită la articolul 3 punctul 3 din Directiva 2008/115/CE;

17. „interdicție de intrare” înseamnă interdicție de intrare astfel cum este definită la articolul 3 punctul 6 din Directiva 2008/115/CE;

18. „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 ([1]) sau infracțiuni echivalente cu acestea în cazul statelor membre care nu au obligații în temeiul directivei respective;

19. „permis de ședere” înseamnă un permis de ședere astfel cum este definit la articolul 2 punctul 16 din Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului ([2]);

20. „viză de lungă ședere” înseamnă o viză de lungă ședere astfel cum se menționează la articolul 18 alineatul (1) din Convenția de punere în aplicare a Acordului Schengen;

21. „amenințare pentru sănătatea publică” înseamnă o amenințare pentru sănătatea publică astfel cum este definită la articolul 2 punctul 21 din Regulamentul (UE) 2016/399.

([1]) 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).

([2]) 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).

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 e 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 din 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 către 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 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 de acces la rețeaua națională 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 (2) 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 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 consecvența dintre copiile naționale și baza de date din SIS; și

(c) operațiunile de inițializare și de restabilire 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) Se alocă fonduri din pachetul financiar de 791 de milioane EUR prevăzut la articolul 5 alineatul (5) litera (b) din Regulamentul (UE) nr. 515/2014 pentru a acoperi costurile aferente punerii în aplicare a prezentului regulament.

(3) Din pachetul financiar menționat la alineatul (2) și fără a aduce atingere finanțării suplimentare în acest scop din alte surse de la bugetul general al Uniunii, suma de 31 098 000 EUR este alocată eu-LISA. Această finanțare este pusă în aplicare în cadrul gestiunii indirecte și contribuie la realizarea dezvoltărilor tehnice necesare în temeiul prezentului regulament în ceea ce privește SIS central și infrastructura de comunicații, precum și la desfășurarea activităților de formare aferente.

(4) Din pachetul financiar menționat la alineatul (2), statele membre care participă la Regulamentul (UE) nr. 515/2014 primesc o finanțare suplimentară globală de 36 810 000 EUR care urmează a fi distribuită în părți egale sub forma unei sume forfetare adăugate alocării de bază. Această finanțare este pusă în aplicare în cadrul gestiunii partajate și este destinată integral actualizării rapide și eficace a sistemelor naționale vizate în conformitate cu cerințele din prezentul regulament.

(5) 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 și biroul SIRENE

(1) Fiecare stat membru desemnează o autoritate (oficiul N.SIS) care deține responsabilitatea principală pentru propriul 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 are răspunderea de a asigura 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, iar respectivele persoane 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 41 alineatul (8).

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 49, 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.

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 62 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 testelor respective sunt luate în considerare ca parte a mecanismului instituit prin Regulamentul (UE) nr. 1053/2013 al Consiliului ([1]).

(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 62 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);

([1]) 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).

(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 profilurile respective la dispoziția autorităților de supraveghere menționate la articolul 55 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 incintelor 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 34.

(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 prin utilizarea datelor dactiloscopice sau al unei imagini faciale în conformitate cu articolul 33, 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.

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 59.

(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.

Programul de formare respectiv 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 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. eu-LISA 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, 7 zile pe săptămână în conformitate cu prezentul regulament, în special în activitatea de întreținere și dezvoltările tehnice necesare pentru buna funcționare a sistemului. Sarcinile respective 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 62 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 profilurile respective 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 posibilitatea că, în cazul unor operațiuni întrerupte, sistemele instalate pot fi readuse la operarea normală (recuperare);

(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); 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 prin utilizarea datelor dactiloscopice sau al imaginilor faciale în conformitate cu articolul 33, 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 înregistrările respective, la cerere, în limitele competenței sale și în scopul îndeplinirii sarcinilor care îi revin.

CAPITOLUL IV

INFORMAREA PUBLICULUI

Articolul 19

Campanii 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

SEMNALĂRILE PENTRU REFUZUL INTRĂRII ȘI AL ȘEDERII PRIVIND RESORTISANȚII ȚĂRILOR TERȚE

Articolul 20

Categoriile de date

(1) Fără a aduce atingere articolului 8 alineatul (1) sau dispozițiilor prezentului regulament care prevăd stocarea de date suplimentare, SIS conține doar categoriile de date care sunt furnizate de fiecare stat membru și care sunt necesare în scopurile prevăzute la articolele 24 și 25.

(2) 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) orice cetățenii 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 48;

(p) dacă persoana vizată este membru de familie al unui cetățean al Uniunii sau o altă persoană care beneficiază de dreptul de liberă circulație, astfel cum se menționează la articolul 26;

(q) dacă decizia de refuz al intrării și al ședерii se bazează pe:

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

(ii) o amenințare gravă pentru securitate, astfel cum se menționează la articolul 24 alineatul (2) litera (b);

(iii) eludarea dreptului Uniunii sau a dreptului intern referitor la intrare și la ședere, astfel cum se menționează la articolul 24 alineatul (2) litera (c);

(iv) o interdicție de intrare, astfel cum se menționează la articolul 24 alineatul (1) litera (b); sau

(v) o măsură restrictivă, astfel cum se menționează la articolul 25;

(r) tipul de infracțiune;

(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) date dactiloscopice;

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

(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, și a standardelor comune menționate la alineatul (4) din prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 62 alineatul (2).

(4) Normele tehnice sunt similare în cazul căutărilor efectuate în CS-SIS, în copiile naționale sau comune și în copiile tehnice efectuate în temeiul articolului 41 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, relevant și important pentru a justifica o semnalare în SIS.

(2) În cazul în care decizia de refuz al intrării și al ședерii menționată la articolul 24 alineatul (1) litera (a) este legată de o infracțiune de terorism, cazul este considerat suficient de adecvat, relevant și 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

Cerințe privind introducerea unei semnalări

(1) Setul minim de date necesare pentru a introduce o semnalare în SIS sunt datele menționate la articolul 20 alineatul (2) literele (a), (g), (k), (m), (n) și (q). Celelalte date menționate la alineatul respectiv sunt introduse la rândul lor în SIS, dacă sunt disponibile.

(2) Datele menționate la articolul 20 alineatul (2) litera (e) din prezentul regulament sunt introduse numai atunci când acest lucru este strict necesar pentru identificarea resortisantului în cauză al unei țări terțe. Atunci când aceste date sunt introduse, statele membre asigură respectarea articolului 9 din Regulamentul (UE) 2016/679.

Articolul 23

Compatibilitatea semnalărilor

(1) Înainte de a introduce o semnalare, statul membru verifică dacă persoana în cauză face deja obiectul unei semnalări în SIS. În acest scop, 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 pentru un stat membru. Dacă este necesar, alte state membre pot introduce noi semnalări referitoare la aceeași persoană, în conformitate cu alineatul (3).

(3) În cazul în care o persoană 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 al 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, 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 din Regulamentul (UE) 2018/1862 se execută cu prioritate, sub rezerva articolului 25 din respectivul regulament.

Articolul 24

Condițiile de introducere a semnalărilor privind refuzul intrării și al șederii

(1) Statele membre introduc o semnalare privind refuzul intrării și al șederii atunci când este îndeplinită una dintre următoarele condiții:

(a) pe baza unei evaluări individuale care include o evaluare a situației personale a resortisantului în cauză al unei țări terțe și a consecințelor refuzului intrării și al șederii acestuia, statul membru a ajuns la concluzia că prezența respectivului resortisant al unei țări terțe pe teritoriul său reprezintă o amenințare pentru ordinea publică sau siguranța publică ori pentru securitatea națională și statul membru, în consecință, a adoptat o decizie administrativă sau hotărâre judecătorească în conformitate cu dreptul său intern de a refuza intrarea și șederea și a emis o semnalare națională privind refuzul intrării și al șederii; sau

(b) statul membru a emis o interdicție de intrare în conformitate cu procedurile care respectă Directiva 2008/115/CE în privința unui resortisant al unei țări terțe.

(2) Situațiile prevăzute la alineatul (1) litera (a) apar atunci când:

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

(b) există motive serioase să se creadă că un resortisant al unei țări terțe a comis o infracțiune gravă, inclusiv o infracțiune de terorism, sau există indicii clare că acesta intenționează să comită o astfel de infracțiune pe teritoriul unui stat membru; sau

(c) un resortisant al unei țări terțe a eludat sau a încercat să eludeze dreptul Uniunii sau dreptul intern referitor la intrarea și șederea pe teritoriul statelor membre.

(3) Statul membru emitent se asigură că semnalarea produce efecte în SIS de îndată ce resortisantul în cauză al unei țări terțe a părăsit teritoriul statelor membre sau cât de curând posibil în cazul în care statul membru emitent a obținut indicații clare asupra faptului că resortisantul țării terțe a părăsit teritoriul statelor membre, pentru a împiedica o nouă intrare a resortisantului respectiv.

(4) Persoanele în privința cărora s-a luat o decizie de refuz al intrării și al șederii astfel cum se menționează la alineatul (1) au dreptul la o cale de atac. Astfel de căi de atac se exercită în conformitate cu dreptul Uniunii și cu dreptul intern care prevăd exercitarea unei căi de atac eficiente în fața unei instanțe.

Articolul 25

Condițiile de introducere a semnalărilor referitoare la resortisanții țărilor terțe cărora li se aplică măsuri restrictive

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

(2) Semnalările se introduc, se actualizează și se șterg de către autoritatea competentă a statului membru care deține președinția Consiliul Uniunii Europene în momentul adoptării măsurii. Dacă respectivul stat membru nu are acces la SIS sau la semnalările introduse în conformitate cu prezentul regulament, responsabilitatea este preluată de statul membru care deține următoarea președinție și care are acces la SIS, inclusiv la semnalările introduse în conformitate cu prezentul regulament.

Statele membre instituie procedurile necesare pentru introducerea, actualizarea și ștergerea unor astfel de semnalări.

Articolul 26

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

(1) Semnalările privind un resortisant al unei țări terțe care beneficiază de dreptul la liberă circulație pe teritoriul Uniunii, în conformitate cu Directiva 2004/38/CE sau în înțelesul unui acord între Uniune sau între Uniune și statele sale membre, pe de o parte, și o țară terță, pe de altă parte, trebuie să fie în conformitate cu normele adoptate pentru punerea în aplicare a directivei sau a acordului respectiv.

(2) În cazul obținerii unui rezultat pozitiv referitor la o semnalare introdusă în conformitate cu articolul 24 cu privire la un resortisant al unei țări terțe care beneficiază de dreptul la liberă circulație pe teritoriul Uniunii, statul membru de executare consultă imediat statul membru emitent, printr-un schimb de informații suplimentare, pentru a stabili fără întârziere acțiunea de urmat.

Articolul 27

Consultarea prealabilă înainte de acordarea sau de prelungirea unui permis de ședere sau a unei vize de lungă ședere

În cazul în care un stat membru are în vedere acordarea sau prelungirea unui permis de ședere sau a unei vize de lungă ședere unui resortisant al unei țări terțe care face obiectul unei semnalări privind refuzul intrării și al șederii introduse de un alt stat membru, statele membre implicate se consultă printr-un schimb de informații suplimentare, în conformitate cu următoarele norme:

(a) statul membru de acordare consultă statul membru emitent înainte de acordarea sau de prelungirea permisului de ședere sau a vizei de lungă ședere;

(b) statul membru emitent răspunde cererii de consultare în termen de 10 zile calendaristice;

(c) lipsa unui răspuns până la termenul prevăzut la litera (b) se interpretează drept lipsa obiecțiilor din partea statului membru emitent cu privire la acordarea sau la prelungirea permisului de ședere sau a vizei de lungă ședere;

(d) atunci când ia decizia în cauză, statul membru de acordare ține seama de motivele care au stat la baza deciziei statului membru emitent și ia în considerare, în conformitate cu dreptul intern, orice amenințare la adresa ordinii publice sau siguranței publice pe care o poate constitui prezența resortisantului în cauză al unei țări terțe pe teritoriul statelor membre;

(e) statul membru de acordare notifică statul membru emitent cu privire la decizia sa; și

(f) în cazul în care statul membru de acordare informează statul membru emitent că intenționează să acorde sau să prelungească permisul de ședere sau viza de lungă ședere sau că a decis să procedeze astfel, statul membru emitent șterge semnalarea privind refuzul intrării și al șederii.

Decizia finală privind acordarea unui permis de ședere sau a unei vize de lungă ședere unui resortisant al unei țări terțe îi revine statului membru de acordare.

Articolul 28

Consultarea prealabilă introducerii unei semnalări privind refuzul intrării și al șederii

În cazul în care un stat membru a luat decizia menționată la articolul 24 alineatul (1) și are în vedere introducerea unei semnalări privind refuzul intrării și al șederii cu privire la resortisantul unei țări terțe care este titularul unui permis de ședere valabil sau al unei vize de lungă ședere valabile acordate de un alt stat membru, statele membre implicate se consultă printr-un schimb de informații suplimentare, în conformitate cu următoarele norme:

(a) statul membru care a luat decizia menționată la articolul 24 alineatul (1) informează statul membru de acordare cu privire la decizie;

(b) schimbul de informații în temeiul literei (a) din prezentul articol include detalii suficiente despre motivele care au stat la baza deciziei menționate la articolul 24 alineatul (1);

(c) pe baza informațiilor furnizate de statul membru care a luat decizia menționată la articolul 24 alineatul (1), statul membru de acordare analizează dacă există motive pentru retragerea permisului de ședere sau a vizei de lungă ședere;

(d) atunci când ia decizia în cauză, statul membru de acordare ține seama de motivele care au stat la baza deciziei statului membru care a luat decizia menționată la articolul 24 alineatul (1) și ia în considerare, în conformitate cu dreptul intern, orice amenințare la adresa ordinii publice sau siguranței publice pe care o poate constitui prezența resortisantului în cauză al unei țări terțe pe teritoriul statelor membre;

(e) în termen de 14 zile calendaristice de la primirea cererii de consultare, statul membru de acordare informează statul membru care a luat decizia menționată la articolul 24 alineatul (1) despre decizia sa sau, în cazul în care nu a fost posibil pentru statul membru de acordare să ia o decizie în acest termen, transmite o solicitare motivată de prelungire în mod excepțional a termenului pentru acordarea unui răspuns cu maximum 12 zile calendaristice suplimentare;

(f) în cazul în care statul membru de acordare notifică statul membru care a luat decizia menționată la articolul 24 alineatul (1) că menține permisul de ședere sau viza de lungă ședere, statul membru care a luat decizia nu introduce semnalarea privind refuzul intrării și al șederii.

Articolul 29

Consultarea ulterioară introducerii unei semnalări privind refuzul intrării și al șederii

În cazul în care se constată că un stat membru a introdus o semnalare privind refuzul intrării și al șederii cu privire la un resortisant al unei țări terțe care este titularul unui permis de ședere valabil sau al unei vize de lungă ședere valabile acordate de un alt stat membru, statele membre implicate se consultă printr-un schimb de informații suplimentare, în conformitate cu următoarele norme:

(a) statul membru emitent informează statul membru de acordare cu privire la semnalarea privind refuzul intrării și al șederii;

(b) schimbul de informații în temeiul literei (a) include suficiente detalii despre motivele semnalării privind refuzul intrării și al șederii;

(c) pe baza informațiilor furnizate de către statul emitent, statul membru de acordare analizează dacă există motive pentru retragerea permisului de ședere sau a vizei de lungă ședere;

(d) atunci când ia decizia în cauză, statul membru de acordare ține seama de motivele care au stat la baza deciziei statului membru emitent și ia în considerare, în conformitate cu dreptul intern, orice amenințare la adresa ordinii publice sau siguranței publice pe care o poate constitui prezența resortisantului în cauză al unei țări terțe pe teritoriul statelor membre;

(e) în termen de 14 zile calendaristice de la primirea cererii de consultare, statul membru de acordare notifică decizia sa statului membru emitent sau, în cazul în care statul membru de acordare nu a putut lua o decizie în acest termen, transmite o solicitare motivată de prelungire în mod excepțional a termenului pentru acordarea unui răspuns cu maximum 12 zile calendaristice suplimentare;

(f) în cazul în care statul membru de acordare notifică statului membru emitent că menține permisul de ședere sau viza de lungă ședere, statul membru emitent șterge imediat semnalarea privind refuzul intrării și al șederii.

Articolul 30

Consultarea în cazul unui rezultat pozitiv cu privire la un resortisant al unei țări terțe care este titularul unui permis de ședere sau al unei vize de lungă ședere valabile

În cazul în care un stat membru obține un rezultat pozitiv referitor la o semnalare privind refuzul intrării și al șederii introdusă de un stat membru în legătură cu un resortisant al unei țări terțe care este titularul unui permis de ședere valabil sau al unei vize de lungă ședere valabile acordate de un alt stat membru, statele membre implicate se consultă printr-un schimb de informații suplimentare, în conformitate cu următoarele norme:

(a) statul membru de executare informează statul membru emitent despre situație;

(b) statul membru emitent inițiază procedura prevăzută la articolul 29;

(c) statul membru emitent informează statul membru de executare despre rezultat în urma consultării.

Decizia privind intrarea resortisantului unei țări terțe este luată de statul membru de executare în conformitate cu Regulamentul (UE) 2016/399.

Articolul 31

Statistici privind schimburile de informații

Statele membre furnizează anual eu-LISA statistici privind schimburile de informații efectuate în conformitate cu articolele 27-30 și privind cazurile în care termenele prevăzute la respectivele articole nu au fost respectate.

CAPITOLUL VI

EFECTUAREA DE CĂUTĂRI PRIN UTILIZAREA DATELOR BIOMETRICE

Articolul 32

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

(1) În SIS se introduc numai fotografiile, imaginile faciale și datele dactiloscopice menționate la articolul 20 alineatul (2) literele (w) și (x) 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 zece amprente digitale prelevate prin rulare. Acestea pot include până la două amprente palmare.

(3) Pentru stocarea datelor biometrice menționate la alineatul (1) din prezentul articol se stabilesc standarde minime de calitate a datelor și specificații tehnice în conformitate cu alineatul (4) 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 persoane în conformitate cu articolul 33 alineatul (1) și pentru utilizarea datelor cu scopul de a identifica o persoană în conformitate cu articolul 33 alineatele (2)-(4).

(4) Comisia adoptă acte de punere în aplicare pentru stabilirea standardelor minime de calitate a datelor și a specificațiilor tehnice menționate la alineatele (1) și (3) din prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 62 alineatul (2).

Articolul 33

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

(1) În cazul în care într-o semnalare în SIS sunt disponibile fotografii, imagini faciale și date dactiloscopice, astfel de fotografii, imagini faciale și date dactiloscopice 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 24 și 25 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 61 pentru a completa prezentul regulament în ceea ce privește stabilirea altor circumstanțe în care se pot utiliza fotografii și imagini faciale pentru identificarea persoanelor.

CAPITOLUL VII

DREPTUL DE ACCES ȘI REEXAMINAREA ȘI ȘTERGEREA SEMNALĂRILOR

Articolul 34

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

(1) Autoritățile naționale competente responsabile cu identificarea resortisanților țărilor terțe 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) 2016/680 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 ([1]), și, după caz, acordarea de consiliere în conformitate cu Regulamentul (CE) nr. 377/2004 al Consiliului ([2]);

(f) examinarea cererilor de viză și luarea deciziilor privind cererile respective, inclusiv privind eventuala anulare, revocare sau prelungire a vizelor, în conformitate cu Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului ([3]).

(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) În sensul articolelor 24 și 25, dreptul de acces la date în SIS și dreptul de a efectua căutări în mod direct în aceste date pot fi exercitate și de către autoritățile judiciare naționale, inclusiv cele responsabile cu inițierea urmăririi penale în cadrul procedurilor penale și cu anchetele judiciare anterioare punerii sub acuzare a unei persoane, în îndeplinirea sarcinilor care le revin, astfel cum se prevede în dreptul intern, precum și de către autoritățile lor coordonatoare.

(4) Dreptul de acces la datele privind documente referitoare la persoane, introduse în conformitate cu articolul 38 alineatul (2) literele (k) și (l) din Regulamentul (UE) 2018/1862, și dreptul de a efectua căutări în aceste date pot fi exercitate, de asemenea, de către autoritățile menționate la alineatul (1) litera (f) din prezentul articol.

(5) Autoritățile competente menționate la prezentul articol sunt incluse în lista menționată la articolul 41 alineatul (8).

Articolul 35

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 solicita informații suplimentare și face schimb de 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 facilitățile 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 sensul prezentului articol se efectuează în conformitate cu regulamentul respectiv.

(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 cu respectarea deplină a dreptului Uniunii în materie de protecție a datelor.

([1]) 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).

([2]) 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).

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

(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 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 menținerea 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 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 aduce atingere la 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 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 este 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 ca fiind 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 ca fiind 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 36

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 34 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 personalul implicat 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 privind 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 ca fiind 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 a accesa date în SIS și de a efectua căutări în acestea. Aceasta nu aduce atingere altor dispoziții din Regulamentul (UE) 2018/1725.

Articolul 37

Evaluarea utilizării SIS de către Europol și de 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 și de către echipele menționate la articolul 36 alineatul (1).

(2) Europol 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 acesteia se transmite Parlamentului European și Consiliului.

Articolul 38

Limitele de acces

Utilizatorii finali, inclusiv Europol 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 39

Perioada de reexaminare a semnalărilor

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

(2) În termen de trei ani de la introducerea unei semnalări în SIS, statul membru emitent reexaminează nevoia de a o păstra. Cu toate acestea, dacă decizia națională pe care se bazează semnalarea prevede o perioadă de valabilitate mai lungă de trei ani, semnalarea se reexaminează în termen de cinci ani.

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

(4) În timpul perioadei de reexaminare, statul membru emitent poate decide, în urma unei evaluări individuale cuprinzătoare care se înregistrează, să păstreze semnalarea 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, alineatul (2) se aplică și prelungirii. Orice astfel de prelungire se comunică CS-SIS.

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

(6) Statele membre întocmesc statistici privind numărul semnalărilor ale căror perioade de păstrare au fost prelungite în conformitate cu alineatul (4) din prezentul articol și le transmit, la cerere, autorităților de supraveghere menționate la articolul 55.

(7) De îndată ce devine clar pentru un birou SIRENE că o semnalare 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 40

Ștergerea semnalărilor

(1) Semnalările privind refuzul intrării și al șederii în temeiul articolului 24 se șterg:

(a) atunci când decizia care a stat la baza acestora a fost retrasă sau anulată de autoritatea competentă; sau

(b) dacă este cazul, în urma procedurii de consultare menționate la articolele 27 și 29.

(2) Semnalările privind resortisanții țărilor terțe cărora li se aplică măsuri restrictive menite să le împiedice intrarea pe teritoriul statelor membre sau tranzitarea acestui teritoriu se șterg atunci când măsura restrictivă a încetat sau când aceasta a fost suspendată ori anulată.

(3) Semnalările privind o persoană care a dobândit cetățenia unui stat membru sau a oricărui stat ai cărui resortisanți beneficiază de dreptul la liberă circulație în temeiul dreptului Uniunii se șterg de îndată ce statul membru emitent ia cunoștință sau este informat în temeiul articolului 44 despre faptul că persoana în cauză a dobândit o astfel de cetățenie.

(4) Semnalările se șterg după expirarea semnalării în conformitate cu articolul 39.

CAPITOLUL VIII

NORME GENERALE DE PRELUCRARE A DATELOR

Articolul 41

Prelucrarea datelor din SIS

(1) Statele membre prelucrează datele menționate la articolul 20 numai în scopul refuzului intrării și al șederii pe teritoriile lor.

(2) Datele sunt copiate numai în scopuri tehnice, atunci când această copiere să fie necesară pentru ca autoritățile competente menționate la articolul 34 să poată efectua o căutare directă. Prezentul regulament se aplică și respectivelor copii. Un stat membru nu copiază datele semnalărilor sau datele suplimentare introduse de un alt stat membru din sistemul său N.SIS sau din CS-SIS în alte fișiere de date naționale.

(3) Copiile tehnice menționate la alineatul (2), care generează baze de date offline se pot păstra maximum 48 de ore.

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

Statele membre țin un inventar actualizat al acestor copii, îl pun la dispoziția autorității 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 34 este autorizat numai în limitele competențelor acestora și numai personalului autorizat în mod corespunzător.

(5) Orice prelucrare a datelor din SIS de către statele membre 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 gravă și iminentă 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) Datele privind documentele referitoare la persoane care sunt introduse în SIS în temeiul articolului 38 alineatul (2) literele (k) și (l) din Regulamentul (UE) 2018/1862 pot fi utilizate de autoritățile competente menționate la articolul 34 alineatul (1) litera (f) în conformitate cu dreptul fiecărui stat membru.

(7) Orice utilizare a datelor din SIS care contravine alineatelor (1)-(6) 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 59.

(8) 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.

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

Articolul 42

Datele din SIS și fișierele naționale

(1) Articolul 41 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 41 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 43

Informații în cazul neexecutării unei semnalări

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

Articolul 44

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 (2), 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 (2), acesta le transmite fără întârziere, printr-un schimb de informații suplimentare, statului membru emitent pentru a permite acestuia din urmă să completeze sau să modifice semnalarea. Datele sunt transmise numai în cazul în care identitatea resortisantului unei țări terțe 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, cât mai curând posibil și în maximum 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 57.

(7) Statele membre fac schimb de informații suplimentare în cazurile 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 47 și la dreptul la o cale de atac în temeiul articolului 54 alineatul (1).

Articolul 45

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 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 și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă se asigură că sunt impuse sancțiuni, în conformitate cu articolul 59.

Articolul 46

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 aceeași persoană.

(2) În cazul în care verificarea încrucișată arată că persoana care face obiectul noii semnalări și 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 47

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 62 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 48

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 62 alineatul (2).

Articolul 49

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 respectivul stat membru a introdus-o sau referitoare 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 50

Transferul datelor cu caracter personal către terți

Datele prelucrate 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 IX

PROTECȚIA DATELOR

Articolul 51

Legislația aplicabilă

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

(2) Regulamentul (UE) 2016/679 se aplică în cazul prelucrării datelor cu caracter personal în temeiul prezentului regulament de către autoritățile competente menționate la articolul 34 din prezentul regulament, 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, în situațiile în care se aplică Directiva (UE) 2016/680.

Articolul 52

Dreptul la informare

(1) Resortisanții țărilor terțe care fac obiectul unei semnalări din SIS sunt informați cu privire la aceasta în conformitate cu articolele 13 și 14 din Regulamentul (UE) 2016/679 sau cu articolele 12 și 13 din Directiva (UE) 2016/680. Această informare se efectuează în scris și este însoțită de o copie a deciziei naționale care a generat semnalarea sau o trimitere la aceasta, astfel cum se menționează la articolul 24 alineatul (1) din prezentul regulament.

(2) Această informare nu se efectuează în cazul în care dreptul intern permite restricționarea dreptului la informare, în special în scopul protejării securității naționale, al apărării, al protejării siguranței publice și al prevenirii, depistării, investigării și urmării penale a infracțiunilor.

Articolul 53

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 la 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 cu privire la 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 proporționată 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, indiferent dacă persoana vizată este într-o țară terță sau nu.

Articolul 54

Căi de atac

(1) Fără a aduce atingere dispozițiilor privind căile de atac din Regulamentul (UE) 2016/679 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 de informații 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 58.

(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 ștergere a 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 o instanță 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 57 alineatul (4).

Articolul 55

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 și 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 56

Supravegherea eu-LISA

(1) Autoritatea Europeană pentru Protecția Datelor este responsabilă cu monitorizarea prelucrării datelor cu caracter personal de către eu-LISA și cu 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 57

Cooperarea dintre autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor

(1) Autoritățile 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 de comun acord alte metode de lucru.

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

CAPITOLUL X

RĂSPUNDEREA ȘI SANCȚIUNILE

Articolul 58

Răspunderea

(1) Fără a aduce atingere dreptului la despăgubiri și răspunderii în temeiul Regulamentului (UE) 2016/679, Directivei (UE) 2016/680 și 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 exonerată de răspundere în temeiul primului paragraf, integral sau parțial, dacă dovedește că nu este responsabilă 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 59

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 XI

DISPOZIȚII FINALE

Articolul 60

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. Astfel de statistici includ statistici privind schimbul de informații în temeiul articolelor 27-31. Statisticile întocmite nu conțin date cu caracter personal. Raportul statistic anual se publică.

(4) Statele membre, Europol 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), (5), (7) și (8).

(5) eu-LISA furnizează Parlamentului European, Consiliului, statelor membre, Comisiei, Europol și 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 să solicite ca 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 se menționează la articolele 11 și 13 din Regulamentul (UE) 2016/1624.

(6) În scopul articolului 15 alineatul (4) și al alineatelor (3), (4) și (5) din prezentul articol, eu-LISA instituie, pune în aplicare și găzduiește în amplasamentele sale tehnice un registru central care conține datele menționate la articolul 15 alineatul (4) și la alineatul (3) din prezentul articol care nu fac posibilă identificarea persoanelor, și care permite Comisiei și agențiilor menționate la alineatul (5) din prezentul articol să obțină rapoarte și statistici specifice. La cerere, eu-LISA acordă statelor membre, Comisiei, Europol 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 un control al accesului și profiluri de utilizator specifice, pentru a se asigura că registrul central este accesat exclusiv în scopul întocmirii de rapoarte și statistici.

(7) La doi ani de la data aplicării prezentului regulament în temeiul articolului 66 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 privind 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.

(8) La trei ani de la data aplicării prezentului regulament în temeiul articolului 66 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 AFIS și a campaniilor de informare privind SIS desfășurate de Comisie în conformitate cu articolul 19.

Raportul de evaluare cuprinde totodată statistici privind numărul semnalărilor introduse în conformitate cu articolul 24 alineatul (1) litera (a) și statistici privind numărul semnalărilor introduse în conformitate cu litera (b) din alineatul respectiv. În ceea ce privește semnalările care intră sub incidența articolului 24 alineatul (1) litera (a), acesta specifică numărul de semnalări introduse în urma situațiilor menționate la articolul 24 alineatul (2) litera (a), (b) sau (c). Raportul de evaluare conține și o evaluare a aplicării articolului 24 de către statele membre.

Comisia transmite raportul de evaluare Parlamentului European și Consiliului.

(9) Comisia adoptă acte de punere în aplicare pentru stabilirea unor norme detaliate privind funcționarea registrului central menționat la alineatul (6) 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 62 alineatul (2).

Articolul 61

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 33 alineatul (4) se conferă Comisiei pe o perioadă nedeterminată de la 27 decembrie 2018.

(3) Delegarea de competențe menționată la articolul 33 alineatul (4) poate fi revocată oricând de Parlamentul European sau de 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 33 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 62

Procedura comitetului

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

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

Articolul 63

Modificarea Regulamentului (CE) nr. 1987/2006

Regulamentul (CE) nr. 1987/2006 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 privind secretul profesional sau alte obligații echivalente de confidențialitate pentru toate persoanele și organismele care lucrează cu date din SIS II și cu 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 activității 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 prezentului regulament, în special cele 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, 7 zile pe săptămână în conformitate cu prezentul regulament, în special în activitatea de întreținere și dezvoltările tehnice 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 prezentului regulament, în special a celor 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 20 alineatul (2) se introduce următoarea literă:

„(ka) tipul infracțiunii;".

6. La articolul 21 se adaugă următorul paragraf:

„În cazul în care decizia de refuz al intrării și al șederii menționată la articolul 24 alineatul (2) este legată 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 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."

7. 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 sunt introduse numai 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 51 alineatul (2).

(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 24 și 26 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."

8. Articolul 26 se înlocuiește cu următorul text:

„*Articolul 26*

Condițiile de introducere a semnalărilor referitoare la resortisanții țărilor terțe cărora li se aplică măsuri restrictive

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

(2) Semnalările se introduc, se actualizează și se șterg de către autoritatea competentă a statului membru care deține președinția Consiliul Uniunii Europene în momentul adoptării măsurii. Dacă respectivul stat membru nu are acces la SIS II sau la semnalări introduse în conformitate cu prezentul regulament, responsabilitatea este preluată de statul membru care deține următoarea președinție și care are acces la SIS II, inclusiv la semnalările introduse în conformitate cu prezentul regulament.

Statele membre instituie procedurile necesare pentru introducerea, actualizarea și ștergerea unor astfel de semnalări."

9. Se introduc următoarele articole:

„*Articolul 27a*

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 (*), are dreptul de a 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 facilitățile 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 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 informatic, nu transferă datele din SIS II 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 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 adecvată, în conformitate cu articolul 14; 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 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. Prezentul regulament 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 ca fiind o descărcare sau o copiere ilegală a datelor din SIS II. Europol nu copiază în alte sisteme ale sale datele semnalărilor sau datele suplimentare care au fost emise de statele membre sau 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 ca fiind o descărcare sau o copiere ilegală a unei 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).

Articolul 27b

Accesul la date în SIS II 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 (**), 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 27 alineatul (1) din prezentul regulament și să fi beneficiat de formarea necesară în conformitate cu articolul 14 din prezentul regulament, 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) cu ajutorul 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 personalul implicat 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 privind 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 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 ca fiind 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 (***).

(*) 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).

(**) 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).

(***) 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 64

Modificarea Convenției de punere în aplicare a Acordului Schengen

Articolul 25 din Convenția de punere în aplicare a Acordului Schengen se elimină.

Articolul 65

Abrogarea

Regulamentul (CE) nr. 1987/2006 se abrogă de la data aplicării prezentului regulament precizată la articolul 66 alineatul (5) primul paragraf.

Trimiterile la regulamentul abrogat se consideră ca fiind trimiteri la prezentul regulament și se citesc în conformitate cu tabelul de corespondență din anexă.

Articolul 66

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) Până la 28 decembrie 2021, Comisia adoptă o decizie prin care stabilește data la care operațiunile SIS intră în funcțiune 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 15 alineatul (7), articolul 19, articolul 20 alineatele (3) și (4), articolul 32 alineatul (4), articolul 33 alineatul (4), articolul 47 alineatul (4), articolul 48 alineatul (6), articolul 60 alineatele (6) și (9), articolul 61, articolul 62, articolul 63 punctele 1-6 și punctul 8, precum și alineatele (3) și (4) din prezentul articol se aplică de la data intrării în vigoare a prezentului regulament;

(b) articolul 63 punctul 9 se aplică de la 28 decembrie 2019;

(c) articolul 63 punctul 7 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	*Pentru Consiliu*
Președintele	*Președintele*
A. TAJANI	K. EDTSTADLER

ANEXĂ

TABEL DE CORESPONDENȚĂ

Regulamentul (CE) nr. 1987/2006	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 32 și 33
Articolul 23	Articolul 22
—	Articolul 23
Articolul 24	Articolul 24
Articolul 25	Articolul 26
Articolul 26	Articolul 25
—	Articolul 27
—	Articolul 28
—	Articolul 29
—	Articolul 30
—	Articolul 31
Articolul 27	Articolul 34
Articolul 27a	Articolul 35
Articolul 27b	Articolul 36
—	Articolul 37
Articolul 28	Articolul 38
Articolul 29	Articolul 39
Articolul 30	Articolul 40
Articolul 31	Articolul 41

Regulamentul (CE) nr. 1987/2006	Prezentul regulament
Articolul 32	Articolul 42
Articolul 33	Articolul 43
Articolul 34	Articolul 44
—	Articolul 45
Articolul 35	Articolul 46
Articolul 36	Articolul 47
Articolul 37	Articolul 48
Articolul 38	Articolul 49
Articolul 39	Articolul 50
Articolul 40	—
—	Articolul 51
Articolul 41	Articolul 53
Articolul 42	Articolul 52
Articolul 43	Articolul 54
Articolul 44	Articolul 55
Articolul 45	Articolul 56
Articolul 46	Articolul 57
Articolul 47	—
Articolul 48	Articolul 58
Articolul 49	Articolul 59
Articolul 50	Articolul 60
—	Articolul 61
Articolul 51	Articolul 62
Articolul 52	—
—	Articolul 63
—	Articolul 64
Articolul 53	—
—	Articolul 65
Articolul 54	—
Articolul 55	Articolul 66