III

(Acte adoptate în temeiul Tratatului UE)

ACTE ADOPTATE ÎN TEMEIUL TITLULUI VI DIN TRATATUL UE

DECIZIA 2007/533/JAI A CONSILIULUI

din 12 iunie 2007

privind înfiinţarea, funcţionarea şi utilizarea Sistemului de informaţii Schengen de a doua generaţie (SIS II)

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind Uniunea Europeană, în special articolul 30 alineatul (1) literele (a) şi (b), articolul 31 alineatul (1) literele (a) şi (b) şi articolul 34 alineatul (2) litera (c),

având în vedere propunerea Comisiei,

având în vedere avizul Parlamentului European [1],

întrucât:

(1) Sistemul de informaţii Schengen („SIS"), înfiinţat în temeiul dispoziţiilor titlului IV din Convenţia din 19 iunie 1990 de punere în aplicare a Acordului Schengen din 14 iunie 1985 dintre guvernele statelor Uniunii Economice Benelux, Republicii Federale Germania şi Republicii Franceze privind eliminarea treptată a controalelor la frontierele comune [2] („Convenţia Schengen"), şi dezvoltarea acestuia, sistemul SIS 1+, constituie un mijloc esenţial de aplicare a dispoziţiilor acquis-ului Schengen, astfel cum au fost integrate în cadrul Uniunii Europene.

(2) Dezvoltarea SIS de a doua generaţie („SIS II") a fost încredinţată Comisiei în temeiul Regulamentului (CE) nr. 2424/2001 al Consiliului [3] şi al Deciziei 2001/886/JAI a Consiliului din 6 decembrie 2001 privind dezvoltarea Sistemului de Informaţii Schengen de a doua generaţie (SIS II) [4]. Sistemul SIS II va înlocui sistemul SIS în conformitate cu Convenţia Schengen.

(3) Prezenta decizie constituie temeiul juridic necesar în vederea reglementării sistemului SIS II în ceea ce priveşte chestiunile care intră în domeniul de aplicare al Tratatului privind Uniunea Europeană („Tratatul UE"). Regulamentul (CE) nr. 1987/2006 al Parlamentului European şi al Consiliului din 20 decembrie 2006 privind înfiinţarea, funcţionarea şi utilizarea Sistemului de informaţii Schengen de a doua generaţie (SIS II) [5] constituie temeiul juridic necesar în vederea reglementării SIS II în ceea ce priveşte chestiunile care intră în domeniul de aplicare al Tratatului de instituire a Comunităţii Europene („Tratatul CE").

(4) Faptul că temeiul juridic necesar pentru reglementarea sistemului SIS II constă în instrumente separate nu afectează principiul potrivit căruia SIS II constituie un sistem de informaţii unic, care ar trebui să funcţioneze ca atare. Prin urmare, anumite dispoziţii ale acestor instrumente ar trebui să fie identice.

(5) SIS II ar trebui să constituie o măsură compensatorie care să contribuie la menţinerea unui grad sporit de securitate în cadrul spaţiului de libertate, securitate şi justiţie al Uniunii Europene, prin sprijinul cooperării operaţionale dintre autorităţile poliţieneşti şi autorităţile judiciare în materie penală.

---

[1] Avizul din 25 octombrie 2006 (nepublicat încă în Jurnalul Oficial).

[2] JO L 239, 22.9.2000, p. 19. Convenţie, astfel cum a fost modificată prin Regulamentul (CE) nr. 1160/2005 al Parlamentului European şi al Consiliului (JO L 191, 22.7.2005, p. 18).

[3] JO L 328, 13.12.2001, p. 4.

[4] JO L 328, 13.12.2001, p. 1.

[5] JO L 381, 28.12.2006, p. 4.

(6) Este necesar să se specifice obiectivele SIS II, arhitectura tehnică şi finanţarea acestuia, să se stabilească norme privind funcţionarea şi utilizarea acestuia şi să se definească responsabilităţile acestuia, categoriile de date care urmează a fi introduse în sistem, scopurile şi criteriile introducerii acestora, autorităţile autorizate să aibă acces la date, interconectarea alertelor şi alte norme privind prelucrarea datelor şi protecţia datelor cu caracter personal.

(7) SIS II urmează să cuprindă un sistem central (SIS II central) şi aplicaţii naţionale. Cheltuielile cu exploatarea sistemului SIS II central şi infrastructura de comunicare aferentă ar trebui să fie suportate din bugetul general al Uniunii Europene.

(8) Este necesar să se impună un manual de stabilire a normelor metodologice privind schimbul anumitor informaţii suplimentare referitoare la acţiunea care trebuie întreprinsă ca urmare a alertelor. Autorităţile naţionale din statele membre ar trebui să asigure schimbul acestor informaţii.

(9) Pentru o perioadă tranzitorie, Comisia ar trebui să fie responsabilă de gestionarea operaţională a sistemului SIS II central şi a unor părţi ale infrastructurii de comunicare. Cu toate acestea, pentru a asigura o tranziţie fără probleme la SIS II, aceasta poate delega parţial sau total responsabilităţile respective către două organisme publice naţionale. Pe termen lung şi ca urmare a unui studiu de impact, incluzând o analiză substanţială a alternativelor din punct de vedere financiar, operaţional şi organizaţional, precum şi a propunerilor legislative ale Comisiei, ar trebui să se instituie o autoritate de gestionare permanentă responsabilă cu aceste sarcini. Perioada tranzitorie nu ar trebui să depăşească cinci ani de la data de la care se aplică prezenta decizie.

(10) SIS II urmează să conţină alerte cu privire la persoanele căutate pentru a fi arestate în vederea predării şi a extrădării. În afară de alerte, este adecvat să se asigure schimbul de informaţii suplimentare, necesar pentru procedurile de predare şi de extrădare. În special, ar trebui să fie prelucrate în cadrul SIS II datele menţionate în articolul 8 din Decizia-cadru 2002/584/JAI din 13 iunie 2002 privind mandatul european de arestare şi procedurile de predare între statele membre ([1]).

(11) Ar trebui să fie posibilă adăugarea la SIS II a unei traduceri a datelor suplimentare, introduse în scopul predării în temeiul mandatului european de arestare şi în scopul extrădării.

(12) SIS II ar trebui să conţină alerte cu privire la persoane dispărute, pentru a asigura protecţia acestora sau pentru a preveni ameninţările la adresa persoanelor căutate în cadrul procedurilor judiciare sau la adresa persoanelor sau a obiectelor supuse controalelor specifice sau controalelor discrete şi la adresa obiectelor căutate pentru a fi confiscate sau folosite ca probe în acţiuni penale.

(13) Alertele nu ar trebui păstrate în SIS II pe o perioadă mai lungă decât cea necesară pentru a îndeplini scopurile pentru care au fost furnizate. Ca regulă generală, alertele privind persoanele ar trebui eliminate în mod automat din SIS II după o perioadă de trei ani. Alertele introduse privind obiectele controalelor discrete sau ale controalelor specifice ar trebui eliminate în mod automat din SIS II după o perioadă de cinci ani. Alertele introduse privind obiectele căutate pentru a fi confiscate sau folosite ca probe în acţiuni penale ar trebui eliminate în mod automat din SIS II după o perioadă de zece ani. Deciziile de a păstra în sistem alerte privind persoanele ar trebui să se bazeze pe o evaluare individuală cuprinzătoare. Statele membre ar trebui să revizuiască alertele cu privire la persoane în termenul stabilit şi să păstreze statistici cu privire la numărul de alerte privind persoanele pentru care s-a prelungit perioada de menţinere în sistem.

(14) SIS II ar trebui să permită prelucrarea datelor biometrice, pentru a facilita identificarea exactă a persoanelor în cauză. În acelaşi scop, SIS II ar trebui, de asemenea, să permită prelucrarea datelor privind persoanele de a căror identitate s-a abuzat, pentru a evita inconvenientele provocate de identificarea greşită a acestora, care face obiectul unor măsuri de garantare adecvate, în special consimţământul persoanei în cauză şi o limitare strictă a scopurilor în care aceste date pot fi prelucrate în mod legal.

(15) Ar trebui să fie posibil ca un stat membru să adauge o indicaţie, denumită reper, la o alertă, astfel încât acţiunea care urmează a fi întreprinsă pe baza alertei să nu fie întreprinsă pe teritoriul său. În cazul în care semnalările sunt emise în vederea arestării sau predării, niciun element al prezentei decizii nu ar trebui interpretat în scopul de a deroga de la dispoziţiile Deciziei-cadru 2002/584/JAI sau de a împiedica aplicarea acestora. Decizia de a adăuga un reper la o alertă ar trebui să se bazeze numai pe motivele de refuz cuprinse în decizia-cadru respectivă.

(16) În cazul în care s-a introdus un reper şi se descoperă locul în care se află o persoană căutată în vederea arestării sau a predării, locul ar trebui comunicat întotdeauna autorităţii judiciare emitente, care poate decide transmiterea mandatului european de arestare autorităţii judiciare competente în conformitate cu dispoziţiile Deciziei-cadru 2002/584/JAI.

(17) Ar trebui să fie posibilă stabilirea de conexiuni de către statele membre între alertele existente în SIS II. Stabilirea de către un stat membru a unor conexiuni între două sau mai multe alerte nu ar trebui să aibă efect asupra acţiunii care urmează a fi întreprinsă, asupra perioadei lor de menţinere în sistem sau asupra dreptului de acces la alerte.

([1]) JO L 190, 18.7.2002, p. 1.

(18) Datele prelucrate în cadrul SIS II în aplicarea prezentei decizii nu ar trebui să fie transferate sau puse la dispoziția țărilor terțe sau a organizațiilor internaționale. Cu toate acestea, este oportună consolidarea cooperării dintre Uniunea Europeană şi Interpol prin promovarea unui schimb eficient de date cuprinse în paşapoarte. În cazul în care datele personale sunt transferate din SIS II către Interpol, aceste date personale ar trebui să aibă un grad de protecție adecvat, garantat printr-un acord care prevede garanții şi condiții stricte.

(19) Toate statele membre au ratificat Convenția Consiliului Europei din 28 ianuarie 1981 privind protecția persoanelor în ceea ce priveşte prelucrarea automată a datelor cu caracter personal. Convenția admite excepții de la drepturile şi obligațiile pe care le prevede, precum şi îngrădiri ale acestora, în anumite limite. Datele cu caracter personal prelucrate în contextul punerii în aplicare a prezentei decizii ar trebui să fie protejate în conformitate cu principiile convenției. Principiile enunțate în convenție ar trebui suplimentate sau clarificate prin prezenta decizie, în cazul în care acest lucru este necesar.

(20) Principiile cuprinse în Recomandarea nr. R (87) 15 a Comitetului Ministerial al Consiliului Europei din 17 septembrie 1987 de reglementare a utilizării datelor cu caracter personal în activitatea poliției ar trebui luată în considerare atunci când datele cu caracter personal sunt prelucrate de către autoritățile polițieneşti în aplicarea prezentei decizii.

(21) Comisia a înaintat Consiliului o propunere de decizie-cadru privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițieneşti şi judiciare în materie penală, care ar trebui aprobată până la finalul anului 2006 şi aplicată prelucrării datelor cu caracter personal care sunt prelucrate în cadrul Sistemului de informații Schengen de a doua generație şi schimbului aferent de informații suplimentare în temeiul prezentei decizii.

(22) Regulamentul (CE) nr. 45/2001 al Parlamentului European şi al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile şi organele comunitare şi privind libera circulație a acestor date [1] şi, în special, părțile privind confidențialitatea şi securitatea prelucrării se aplică prelucrării datelor cu caracter personal de către instituțiile şi organismele comunitare în îndeplinirea sarcinilor lor ca autorități responsabile cu gestionarea operațională a SIS II în exercitarea activităților care intră, total sau parțial, în domeniul de aplicare a dreptului comunitar. Prelucrarea datelor cu caracter personal din SIS II intră parțial în domeniul de aplicare a dreptului comunitar. Aplicarea consecventă şi uniformă a normelor privind protecția drepturilor şi libertăților fundamentale ale persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal necesită clarificarea potrivit căreia, în cazul în care Comisia prelucrează date cu caracter personal în aplicarea prezentei decizii, se aplică Regulamentul (CE) nr. 45/2001. Principiile enunțate în Regulamentul (CE) nr. 45/2001 ar trebui suplimentate sau clarificate prin prezenta decizie, în cazul în care acest lucru este necesar.

(23) În ceea ce priveşte confidențialitatea, dispozițiile corespunzătoare ale Statutului funcționarilor Comunităților Europene şi regimul care se aplică celorlalți agenți ai Comunităților Europene ar trebui să se aplice în cazul funcționarilor şi al celorlalți agenți angajați şi care îşi desfăşoară activitatea în legătură cu SIS II.

(24) Se cuvine ca autoritățile naționale de control să monitorizeze legalitatea prelucrării datelor cu caracter personal de către statele membre, în timp ce Autoritatea Europeană pentru Protecția Datelor, desemnată în conformitate cu Decizia 2004/55/CE a Parlamentului European şi a Consiliului din 22 decembrie 2003 de desemnare a organismului de supraveghere independent prevăzut la articolul 286 din Tratatul CE [2], ar trebui să monitorizeze activitățile instituțiilor şi ale organismelor comunitare referitoare la prelucrarea datelor cu caracter personal, având în vedere sarcinile limitate ale instituțiilor şi ale organismelor comunitare în ceea ce priveşte datele ca atare.

(25) Atât statele membre, cât şi Comisia ar trebui să elaboreze un plan de securitate pentru a facilita punerea în aplicare a obligațiilor privind securitatea şi ar trebui să coopereze între ele pentru a aborda chestiunile legate de securitate dintr-o perspectivă comună.

(26) Dispozițiile Convenției din 26 iulie 1995 privind constituirea Oficiului European de Poliție [3] (denumită în continuare „Convenția Europol") cu privire la protecția datelor se aplică prelucrării datelor din SIS II de către Europol, inclusiv cele privind competențele organismului de control comun, înființat în temeiul Convenției Europol, de monitorizare a activităților acestui oficiu şi cele privind responsabilitatea care decurge din orice prelucrare ilegală a datelor de către Europol.

(27) Dispozițiile Deciziei 2002/187/JAI din 28 februarie 2002 de constituire a Eurojust în scopul consolidării luptei împotriva formelor grave de criminalitate [4] cu privire la protecția datelor se aplică prelucrării datelor din SIS II de către Eurojust, inclusiv cele privind competențele organismului de control comun, înființat în temeiul deciziei respective, de monitorizare a activităților acestui oficiu şi cele privind responsabilitatea care decurge din orice prelucrare ilegală a datelor de către Eurojust.

[1] JO L 8, 12.1.2001, p. 1.

[2] JO L 12, 17.1.2004, p. 47.

[3] JO C 316, 27.11.1995, p. 2.

[4] JO L 63, 6.3.2002, p. 1.

(28) Pentru a asigura transparența, un raport privind funcționarea sistemului SIS II central şi a infrastructurii de comunicare, inclusiv securitatea acesteia, precum şi schimbul de informații suplimentare, ar trebui redactat o dată la doi ani de către Comisie ori de către autoritatea de gestionare, după înființarea acesteia. Comisia ar trebui să emită o evaluare completă o dată la patru ani.

(29) Din motive ce țin de natura lor tehnică, de gradul lor de precizie şi de nevoia lor de actualizare constantă, anumite aspecte ale SIS II, cum ar fi normele tehnice cu privire la introducerea datelor, inclusiv a datelor necesare pentru introducerea unei alerte, pentru actualizarea, eliminarea sau căutarea datelor, normele privind compatibilitatea şi prioritatea alertelor, adăugarea de repere, conexiunile dintre alerte şi schimbul de informații suplimentare, nu pot fi reglementate în mod exhaustiv de dispozițiile prezentei decizii. Prin urmare, competențele de executare cu privire la aceste aspecte ar trebui delegate Comisiei. Normele tehnice privind căutarea alertelor ar trebui să ia în considerare funcționarea fără probleme a aplicațiilor naționale. Sub rezerva unui studiu de impact al Comisiei, ar trebui să se decidă măsura în care măsurile de punere în aplicare ar putea intra în sfera responsabilităților autorității de gestionare, odată ce aceasta este înființată.

(30) Prezenta decizie ar trebui să definească procedura de adoptare a măsurilor necesare în vederea punerii în aplicare a acesteia. Procedura de adoptare a măsurilor de punere în aplicare în temeiul prezentei decizii şi procedura de adoptare a măsurilor de punere în aplicare în temeiul Regulamentului (CE) nr. 1987/2006 ar trebui să fie una şi aceeaşi.

(31) Este oportună stabilirea unor dispoziții tranzitorii cu privire la alertele emise în cadrul SIS 1+ care urmează să fie transferate în SIS II. Anumite dispoziții ale acquis-ului Schengen ar trebui să continue să se aplice pentru o perioadă limitată, până la examinarea de către statele membre a compatibilității alertelor respective cu noul cadru legal. Compatibilitatea alertelor cu privire la persoane ar trebui examinată prioritar. De asemenea, orice modificare, adăugare, corecție sau actualizare a unei alerte transferate din SIS 1+ în SIS II, precum şi orice rezultat al unei astfel de alerte ar trebui să declanşeze fără întârziere o examinare a compatibilității acesteia cu dispozițiile prezentei decizii.

(32) Este necesar să se stabilească dispoziții speciale privind partea din buget alocată operațiunilor desfăşurate în cadrul SIS şi care nu face parte din bugetul general al Uniunii Europene.

(33) Întrucât obiectivele acțiunii care trebuie întreprinse, şi anume stabilirea şi reglementarea unui sistem de informare comun, nu pot fi realizate în mod satisfăcător de către statele membre şi, având în vedere amploarea şi efectele acțiunii, pot fi realizate mai bine la nivelul Uniunii Europene, Consiliul poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul CE şi menționat la articolul 2 din Tratatul UE. Prezenta decizie nu depăşeşte ceea ce este necesar pentru a îndeplini aceste obiective, în conformitate cu principiul proporționalității, astfel cum este enunțat la articolul 5 din Tratatul CE.

(34) Prezenta decizie respectă drepturile fundamentale şi observă principiile consacrate în special de Carta Drepturilor Fundamentale ale Uniunii Europene.

(35) Regatul Unit participă la adoptarea și aplicarea prezentei decizii, în conformitate cu articolul 5 din Protocolul de integrare a acquis-ului Schengen în cadrul Uniunii Europene, anexat la Tratatul UE şi la Tratatul CE, precum şi cu articolul 8 alineatul (2) din Decizia 2000/365/CE a Consiliului din 29 mai 2000 privind solicitarea Regatului Unit al Marii Britanii şi Irlandei de Nord de a participa la unele dintre dispozițiile acquis-ului Schengen [1].

(36) Irlanda participă la adoptarea și aplicarea prezentei decizii, în conformitate cu articolul 5 din Protocolul de integrare a acquis-ului Schengen în cadrul Uniunii Europene anexat la Tratatul UE şi la Tratatul CE, precum şi cu articolul 6 alineatul (2) din Decizia 2002/192/CE a Consiliului din 28 februarie 2002 privind solicitarea Irlandei de a participa la unele dintre dispozițiile acquis-ului Schengen [2].

(37) Prezenta decizie nu aduce atingere măsurilor destinate participării parțiale a Regatului Unit şi a Irlandei la acquis-ul Schengen, în conformitate cu Deciziile 2000/365/CE, respectiv 2002/192/CE.

(38) În ceea ce priveşte Islanda şi Norvegia, prezenta decizie reprezintă o dezvoltare a dispozițiilor acquis-ului Schengen în sensul Acordului încheiat de Consiliul Uniunii Europene, Republica Islanda şi Regatul Norvegiei privind asocierea acestora din urmă la transpunerea, punerea în aplicare şi dezvoltarea acquis-ului Schengen [3], dispoziții care intră în domeniul de aplicare menționat la articolul 1 punctul G din Decizia 1999/437/CE a Consiliului [4] privind anumite modalități de aplicare a respectivului acord.

(39) Ar trebui să se încheie un acord care să permită reprezentanților Islandei şi Norvegiei asocierea la activitatea comitetelor care sprijină Comisia în exercitarea competențelor de execuție ale acesteia. O astfel de măsură a fost preconizată în schimbul de scrisori dintre Consiliul Uniunii Europene şi Republica Islanda şi Regatul Norvegiei cu privire la comitetele care oferă asistență Comisiei Europene pentru exercitarea atribuțiilor sale executive [5], anexate la acordul menționat anterior.

---

[1] JO L 131, 1.6.2000, p. 43.
[2] JO L 64, 7.3.2002, p. 20.
[3] JO L 176, 10.7.1999, p. 36.
[4] JO L 176, 10.7.1999, p. 31.
[5] JO L 176, 10.7.1999, p. 53.

(40) În ceea ce priveşte Elveţia, prezenta decizie reprezintă o dezvoltare a dispoziţiilor acquis-ului Schengen în sensul Acordului încheiat între Uniunea Europeană, Comunitatea Europeană şi Confederaţia Elveţiană privind asocierea acesteia din urmă la transpunerea, punerea în aplicare şi dezvoltarea acquis-ului Schengen, dispoziţii care intră în domeniul de aplicare menţionat la articolul 1 punctul G din Decizia 1999/437/CE a Consiliului din 17 mai 1999, coroborat cu articolul 4 alineatul (1) din Decizia 2004/849/CE a Consiliului [1] şi din Decizia 2004/860/CE [2].

(41) Ar trebui să se încheie un acord care să permită reprezentanţilor Elveţiei asocierea la activitatea comitetelor care sprijină Comisia în exercitarea competenţelor sale de executare. Un astfel de cadru a fost preconizat în schimbul de scrisori dintre Comunitate şi Elveţia, anexat la acordul sus-menţionat.

(42) Prezenta decizie reprezintă un act întemeiat pe acquis-ul Schengen sau care se raportează la acesta în sensul articolului 3 alineatul (2) din Actul de aderare din 2003 şi al articolului 4 alineatul (2) din Actul de aderare din 2005.

(43) Prezenta decizie ar trebui să se aplice Regatului Unit, Irlandei şi Elveţiei, la date hotărâte în conformitate cu procedurile stabilite în documentele corespunzătoare privind aplicarea acquis-ului Schengen în cazul acelor state,

DECIDE:

CAPITOLUL I

DISPOZIŢII GENERALE

Articolul 1

Înfiinţarea şi obiectivul general al sistemului SIS II

(1) Se înfiinţează prin prezenta Sistemul de informaţii Schengen de a doua generaţie („SIS II”).

(2) Scopul SIS II este, în conformitate cu prezenta decizie, acela de a asigura un grad sporit de securitate în cadrul spaţiului de libertate, securitate şi justiţie al Uniunii Europene, inclusiv menţinerea securităţii şi a ordinii publice şi garantarea securităţii pe teritoriul statelor membre, precum şi de a aplica dispoziţiile părţii a treia titlul IV din Tratatul CE, referitoare la deplasarea persoanelor pe teritoriul acestora, cu ajutorul informaţiilor comunicate prin intermediul acestui sistem.

Articolul 2

Domeniul de aplicare

(1) Prezenta decizie stabileşte condiţiile şi procedurile de introducere în SIS II şi de prelucrare a alertelor privind persoanele şi obiectele, de schimb al datelor şi al informaţiilor suplimentare în scopul cooperării judiciare şi poliţieneşti în materie penală.

(2) Prezenta decizie stabileşte, de asemenea, dispoziţii privind arhitectura tehnică a sistemului SIS II, responsabilităţile statelor membre şi ale autorităţii de gestionare menţionate la articolul 15, prelucrarea datelor cu caracter general, drepturile persoanelor interesate şi responsabilitatea.

Articolul 3

Definiţii

(1) În sensul prezentei decizii, se aplică următoarele definiţii:

(a) „alertă” înseamnă o serie de date introduse în SIS II care le permite autorităţilor competente să identifice o persoană sau un obiect în vederea luării unor măsuri specifice în ceea o/îl priveşte;

(b) „informaţii suplimentare” înseamnă acele informaţii care nu sunt stocate în SIS II, dar care sunt în legătură cu alertele introduse în SIS II şi care urmează a fi transmise în cadrul schimbului de informaţii:

(i) pentru a permite statelor membre să se consulte sau să se informeze reciproc în cazul în care introduc o alertă;

(ii) în urma obţinerii unui rezultat, pentru a permite luarea unei măsuri adecvate;

(iii) în cazul în care măsura necesară nu poate fi luată;

(iv) în cazul în care se ia în considerare calitatea datelor din SIS II;

(v) în cazul în care se ia în considerare compatibilitatea alertelor unele cu altele şi prioritatea acestora;

(vi) în cazul în care se iau în considerare drepturile de acces;

(c) „date suplimentare” înseamnă datele stocate în SIS II şi care sunt în legătură cu alertele din SIS II, date care urmează să fie puse, fără întârziere, la dispoziţia autorităţilor competente, în cazul în care o persoană cu privire la care s-au introdus date în SIS II este găsită ca urmare a căutărilor efectuate în acest sistem;

[1] Decizia 2004/849/EC a Consiliului din 25 octombrie 2004 privind semnarea, în numele Uniunii Europene, şi aplicarea provizorie a anumitor dispoziţii ale Acordului dintre Uniunea Europeană, Comunitatea Europeană şi Confederaţia Elveţiană referitoare la asocierea Confederaţiei Elveţiene la transpunerea, punerea în aplicare şi dezvoltarea acquis-ului Schengen (JO L 368, 15.12.2004, p. 26).

[2] Decizia 2004/860/CE a Consiliului din 25 octombrie 2004 privind semnarea, în numele Comunităţii Europene, şi aplicarea provizorie a anumitor dispoziţii ale Acordului dintre Uniunea Europeană, Comunitatea Europeană şi Confederaţia Elveţiană referitoare la asocierea Confederaţiei Elveţiene la punerea în aplicare, asigurarea respectării şi dezvoltarea acquis-ului Schengen (JO L 370, 17.12.2004, p. 78).

(d) „date cu caracter personal" înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană identificabilă este o persoană care poate fi identificată, în mod direct sau indirect;

(e) „prelucrarea datelor cu caracter personal" („prelucrarea"): orice operațiune sau set de operațiuni efectuate cu privire la datele cu caracter personal, indiferent dacă se realizează prin mijloace automate sau nu, precum colectarea, înregistrarea, organizarea, stocarea, adaptarea sau modificarea, recuperarea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în alt mod, alinierea sau combinarea, blocarea, ştergerea sau distrugerea datelor.

(2) Se consideră că orice trimitere făcută în cadrul prezentei decizii la dispozițiile Deciziei-cadru 2002/584/JAI include dispozițiile corespunzătoare din acordurile încheiate între Uniunea Europeană şi țări terțe în temeiul articolelor 24 şi 38 din Tratatul UE în scopul predării persoanelor pe baza unui mandat de arestare, care prevăd transmiterea unui astfel de mandat de arestare prin intermediul Sistemului de Informații Schengen.

Articolul 4

Arhitectura tehnică şi modurile de funcționare a sistemului SIS II

(1) SIS II este compus din următoarele elemente:

(a) un sistem central („SIS II central") compus din:

— o funcție de suport tehnic („CS-SIS") care conține o bază de date, „baza de date SIS II";

— o interfață națională uniformă („NI-SIS");

(b) un sistem național („N.SIS II") în fiecare dintre statele membre, care constă în sistemele naționale de date care comunică cu SIS II central. Un sistem N.SIS II poate conține un fişier de date (o „copie națională") care conține o copie completă sau parțială a bazei de date SIS II;

(c) o infrastructură de comunicare între CS-SIS şi NI-SIS („infrastructura de comunicare") care asigură o rețea virtuală criptată consacrată datelor din SIS II şi schimbului de date între birourile SIRENE, în conformitate cu articolul 7 alineatul (2).

(2) Datele din SIS II sunt introduse, actualizate, eliminate şi căutate prin intermediul diverselor sisteme N.SIS II. O copie națională este accesibilă pentru efectuarea de căutări automate pe teritoriul fiecărui stat membru care foloseşte o astfel de copie. Operațiunea de căutare în fişierele de date ale sistemelor N.SIS II ale celorlalte state membre nu este posibilă.

(3) Sistemul CS-SIS, care efectuează controlul tehnic şi îndeplineşte funcții administrative, se stabileşte la Strasbourg (Franța), iar un sistem CS-SIS de rezervă, capabil să preia toate funcțiile sistemului CS-SIS în cazul căderii acestuia, se stabileşte la Sankt Johann im Pongau (Austria).

(4) CS-SIS asigură serviciile necesare pentru introducerea şi prelucrarea datelor din SIS II, inclusiv pentru căutările din baza de date SIS II. Pentru statele membre care utilizează o copie națională, CS-SIS:

(a) asigură actualizarea online a copiilor naționale;

(b) asigură sincronizarea şi consecvența dintre copiile naționale şi baza de date a sistemului SIS II;

(c) asigură operațiunile de inițializare şi de restabilire a copiilor naționale.

Articolul 5

Costurile

(1) Costurile aferente înființării, funcționării şi întreținerii sistemului SIS II central şi infrastructurii de comunicare sunt suportate din bugetul general al Uniunii Europene.

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

(3) Costurile aferente înființării, funcționării şi întreținerii sistemului N.SIS II sunt suportate de către statele membre implicate.

CAPITOLUL II

RESPONSABILITĂȚILE STATELOR MEMBRE

Articolul 6

Sistemele naționale

Fiecare stat membru este responsabil cu înființarea, funcționarea şi întreținerea propriului sistem N.SIS II şi cu conectarea sistemului său N.SIS II la NI-SIS.

Articolul 7

Oficiul N.SIS II şi biroul SIRENE

(1) Fiecare stat membru desemnează o autoritate („oficiul N.SIS II") care îşi asumă responsabilitatea principală pentru sistemul N.SIS II al acelui stat.

Autoritatea respectivă poartă răspunderea pentru buna funcționare şi pentru securitatea sistemului N.SIS II, asigură accesul autorităților competente la sistemul SIS II şi ia măsurile necesare pentru a asigura respectarea dispozițiilor prezentei decizii.

Fiecare stat membru îşi transmite alertele prin intermediul propriului oficiu N.SIS II.

(2) Fiecare stat membru îşi desemnează autoritatea care asigură schimbul tuturor informaţiilor suplimentare („biroul SIRENE") în conformitate cu dispoziţiile Manualului SIRENE, menţionate la articolul 8.

Birourile respective coordonează, de asemenea, verificarea calităţii informaţiilor introduse în SIS II. În acest scop, acestea au acces la datele prelucrate în cadrul SIS II.

(3) Statele membre informează autoritatea de gestionare a oficiului N.SIS II propriu şi a biroului SIRENE propriu. Autoritatea de gestionare publică lista acestora, împreună cu lista menţionată la articolul 46 alineatul (8).

Articolul 8

Schimbul de informaţii suplimentare

(1) Schimbul de informaţii suplimentare se face în conformitate cu dispoziţiile Manualului SIRENE şi ale infrastructurii de comunicare. În cazul în care infrastructura de comunicare nu este accesibilă, statele membre pot folosi alte mijloace tehnice, securizate în mod corespunzător, pentru schimbul de informaţii suplimentare.

(2) Informaţiile suplimentare se utilizează numai în scopul în care au fost transmise.

(3) Cererilor de informaţii suplimentare depuse de către alte state membre li se dă un răspuns cât mai repede posibil.

(4) Normele pentru schimbul de informaţii suplimentare se stabilesc în conformitate cu procedura menţionată la articolul 67 sub forma unui manual numit „Manualul SIRENE", fără a aduce atingere dispoziţiilor instrumentului de constituire a autorităţii de gestionare.

Articolul 9

Conformitatea tehnică

(1) Pentru a asigura o transmisie rapidă şi eficientă a datelor, fiecare stat membru respectă, la crearea propriului N.SIS II, protocoalele şi procedurile tehnice stabilite pentru a asigura compatibilitatea propriului N-SIS II cu CS-SIS. Aceste protocoale şi proceduri tehnice se stabilesc în conformitate cu procedura menţionată la articolul 67, fără a aduce atingere dispoziţiilor instrumentului de constituire a autorităţii de gestionare.

(2) În cazul în care un stat membru foloseşte o copie naţională, acesta asigură, prin intermediul serviciilor furnizate de CS-SIS, că datele stocate în copia naţională sunt identice şi consecvente cu baza de date SIS II prin efectuarea actualizărilor automate menţionate la articolul 4 alineatul (4) şi că o consultare a copiei sale naţionale generează un rezultat echivalent cu cel al unei consultări a bazei de date SIS II.

Articolul 10

Securitatea – Statele membre

(1) Fiecare stat membru se angajează, în legătură cu propriul N.SIS II, să adopte măsurile necesare, inclusiv un plan de securitate, pentru:

(a) a proteja fizic datele, inclusiv prin întocmirea unor planuri pentru situaţii neprevăzute în vederea protecţiei infrastructurii critice;

(b) a împiedica accesul persoanelor neautorizate la zonele de prelucrare a datelor cu caracter personal (controlul accesului în astfel de zone);

(c) a preveni citirea, copierea, modificarea sau eliminarea suportului de date în mod neautorizat (controlul suportului de date);

(d) a preveni introducerea neautorizată de date şi inspectarea, modificarea sau ştergerea neautorizată a datelor cu caracter personal (controlul stocării);

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

(f) a asigura că persoanele autorizate să utilizeze un sistem de prelucrare automată a datelor au acces numai la datele pentru care deţin autorizaţia de acces prin intermediul unei identităţi unice şi individuale de utilizator şi al unui mod de acces confidenţial (controlul accesului la date);

(g) a asigura faptul că toate autorităţile care au acces la SIS II sau la facilităţile de prelucrare a datelor creează profiluri care descriu funcţiunile şi responsabilităţile persoanelor cu autorizaţie de acces, introducere, actualizare, ştergere şi căutare a datelor şi pun fără întârziere aceste profiluri la dispoziţia autorităţilor naţionale de control menţionate la articolul 60, la cererea acestora din urmă (profiluri personale);

(h) a se asigura că este posibil să verifice şi să stabilească organismele cărora le pot fi transmise datele cu caracter personal folosind echipamentele de comunicaţii (controlul comunicaţiilor);

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

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

(k) a monitoriza eficacitatea măsurilor de securitate menţionate în prezentul alineat şi a lua măsurile de organizare necesare referitoare la monitorizarea internă pentru a asigura conformitatea cu prezenta decizie (autoauditare).

(2) Statele membre iau măsurile echivalente celor menționate în alineatul (1) referitoare la securitate în ceea ce privește schimbul de informații suplimentare.

Articolul 11

Confidențialitatea – Statele membre

Fiecare stat membru aplică propriile norme în domeniul secretului profesional sau alte obligații echivalente de confidențialitate pentru toate persoanele și organismele care lucrează cu date din SIS II și alte informații suplimentare, în conformitate cu legislația națională. Această obligație subzistă chiar și după încetarea mandatului sau a contractului de muncă al persoanelor respective sau după încetarea activităților organismelor respective.

Articolul 12

Păstrarea înregistrărilor la nivel național

(1) Statele membre care nu folosesc copii naționale se asigură că toate accesările și toate schimburile de date personale în cadrul CS-SIS sunt înregistrate în propriul N.SIS II, în scopul verificării legalității căutării, monitorizării legalității procesării datelor, automonitorizării și asigurării funcționării corespunzătoare a N.SIS II, precum și a integrității și securității datelor.

(2) Statele membre care folosesc copii naționale asigură că toate accesările și schimburile de date din SIS II sunt înregistrate în scopul menționat la alineatul (1). Aceasta nu se aplică proceselor menționate la articolul 4 alineatul (4).

(3) Înregistrările arată, în special, istoricul alertelor, data și ora transmisiei de date, datele folosite pentru efectuarea unei căutări, o referință cu privire la datele transmise, precum și numele atât al autorității competente, cât și al persoanei responsabile cu procesarea datelor.

(4) Înregistrările pot fi folosite doar în scopurile menționate la alineatele (1) și (2) și se șterg după cel puțin un an și cel mult trei ani de la creare. Înregistrările care includ istoricul alertelor pot fi șterse între unu și trei ani de la ștergerea alertelor.

(5) Înregistrările pot fi păstrate mai mult timp, dacă sunt necesare pentru procedurile de monitorizare care se află deja în curs de desfășurare.

(6) Autoritățile naționale competente responsabile cu verificarea legalității căutărilor, monitorizarea legalității procesării datelor, automonitorizarea și asigurarea funcționării corespunzătoare a N.SIS II, precum și cu integritatea și securitatea datelor au acces, în limitele competenței și la solicitarea acestora, la aceste înregistrări în scopul îndeplinirii obligațiilor ce le revin.

Articolul 13

Automonitorizarea

Statele membre asigură că fiecare autoritate care are dreptul să acceseze datele SIS II ia măsurile necesare pentru asigurarea conformității cu prezenta decizie și cooperează, atunci când este necesar, cu autoritatea națională de control.

Articolul 14

Pregătirea personalului

Înainte de a fi autorizat să proceseze datele stocate în SIS II, personalul autorităților care are dreptul să acceseze SIS II va beneficia de pregătirea corespunzătoare în domeniul securității datelor și al normelor de protecție a datelor, fiind informat cu privire la toate infracțiunile și sancțiunile aplicabile.

CAPITOLUL III

RESPONSABILITĂȚILE AUTORITĂȚII DE GESTIONARE

Articolul 15

Gestionarea operațională

(1) După o perioadă de tranziție, autoritatea de gestionare („autoritatea de gestionare”), finanțată de la bugetul general al Uniunii Europene, este responsabilă de gestionarea operațională a SIS II central. Autoritatea de gestionare asigură, în cooperare cu statele membre, faptul că SIS II central dispune în orice moment de cea mai bună tehnologie existentă, sub rezerva unei analize cost-beneficiu.

(2) Autoritatea de gestionare este responsabilă, de asemenea, și cu următoarele sarcini care țin de infrastructura de comunicare:

(a) supraveghere;

(b) securitate;

(c) coordonarea relațiilor dintre statele membre și furnizor.

(3) Comisia este responsabilă de toate celelalte sarcini care țin de infrastructura de comunicare, în special cu:

(a) sarcini referitoare la execuția bugetară;

(b) achiziții și reînnoire;

(c) chestiuni contractuale.

(4) În timpul perioadei de tranziție, înainte ca autoritatea de gestionare să își preia responsabilitățile, Comisia este responsabilă cu gestionarea operațională a SIS II central. Comisia poate delega organismelor din sectorul public național din două țări diferite această sarcină și sarcinile care țin de punerea în aplicare a bugetului în conformitate cu Regulamentul (CE, Euratom) nr. 1605/2002 al Consiliului din 25 iunie 2002 privind regulamentul financiar aplicabil bugetului general al Comunităților Europene [1].

(5) Fiecare organism public național, în conformitate cu dispozițiile alineatului (4), trebuie să corespundă în special următoarelor criterii de selecție:

(a) trebuie să demonstreze că are o experiență îndelungată în operarea unui sistem informațional la scară largă cu funcționalitățile menționate la articolul 4 alineatul (4);

(b) trebuie să dețină un nivel înalt de expertiză în domeniul serviciilor și imperativelor de securitate adiacente unui sistem informațional cu funcționalități comparabile cu cele menționate la articolul 4 alineatul (4);

(c) trebuie să dispună de personal suficient și experimentat care să posede experiența profesională corespunzătoare și capacitățile lingvistice necesare lucrului într-un mediu de cooperare la nivel internațional cum este SIS II;

(d) trebuie să dețină o infrastructură sigură și special gândită, capabilă, în special, să susțină și să garanteze funcționarea constantă a sistemelor informaționale de mari dimensiuni; și

(e) mediul său administrativ trebuie să permită buna îndeplinire a sarcinilor sale și evitarea oricărui conflict de interese.

(6) Înainte de orice delegare, în sensul dispozițiilor alineatului (4) și la intervale regulate după aceea, Comisia informează Parlamentul European și Consiliul referitor la termenii delegării, la domeniul ei strict de aplicare și la organismele cărora li s-au delegat sarcini.

(7) În cazurile în care Comisia deleagă responsabilitățile care îi revin în cursul perioadei tranziționale în temeiul alineatului (4), aceasta trebuie să asigure ca această delegare respectă în totalitate limitele stabilite de sistemul instituțional prevăzute în Tratatul CE. Ea se asigură, în special, că respectiva delegare nu influențează în mod negativ mecanismele efective de control exercitate, în conformitate cu dreptul comunitar, de Curtea de Justiție, Curtea de Conturi sau Autoritatea Europeană pentru Protecția Datelor.

(8) Gestionarea operațională a SIS II central constă în toate sarcinile necesare menținerii SIS II central în funcțiune 24 de ore pe zi, șapte zile pe săptămână în conformitate cu prezenta decizie, în special activitatea de întreținere și evoluția tehnică necesare pentru buna funcționare a sistemului.

[1] JO L 248, 16.9.2002, p. 1.

Articolul 16

Securitatea

(1) Autoritatea de gestionare, în ceea ce privește SIS II central și, respectiv, Comisia, în ceea ce privește infrastructura de comunicare, adoptă măsurile necesare, inclusiv cele ale unui plan de securitate, pentru:

(a) a proteja fizic datele, inclusiv prin întocmirea unor planuri pentru situații neprevăzute în vederea protecției infrastructurii critice;

(b) a împiedica accesul persoanelor neautorizate la zonele de prelucrare a datelor cu caracter personal (controlul accesului în astfel de zone);

(c) a preveni citirea, copierea, modificarea sau eliminarea suportului de date în mod neautorizat (controlul suportului de date);

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

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

(f) a 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 intermediul unei identități unice și individuale de utilizator și al unui mod de acces confidențial (controlul accesului la date);

(g) a crea profile care descriu funcțiile și responsabilitățile persoanelor care sunt autorizate să acceseze datele sau zonele de procesare a datelor și să pună aceste profiluri la dispoziția Autorității Europene pentru Protecția Datelor menționate la articolul 61, fără întârziere, atunci când acesta o solicită (profiluri personale);

(h) a se asigura că este posibil să verifice și să stabilească organismele cărora le pot fi transmise datele cu caracter personal folosind echipamentele de comunicații (controlul comunicațiilor);

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

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

(k) a monitoriza eficacitatea măsurilor de securitate menționate în prezentul alineat și a lua măsurile de organizare necesare referitoare la monitorizarea internă pentru a asigura conformitatea cu prezenta decizie (autoauditare).

(2) Autoritatea de gestionare ia măsurile echivalente celor menționate la alineatul (1) referitoare la securitate în ceea ce privește schimbul de informații suplimentare prin infrastructura de comunicare.

Articolul 17

Confidențialitatea – Autoritatea de gestionare

(1) Fără a aduce atingere articolului 17 din Statutul funcționarilor Comunităților Europene, autoritatea de gestionare aplică normele corespunzătoare privind secretul profesional sau alte responsabilități echivalente de confidențialitate la standarde comparabile celor stipulate la articolul 11 din prezenta decizie tuturor angajaților care lucrează cu date SIS II. Această obligație subzistă chiar și după încetarea mandatului, a contractului de muncă sau după încetarea activităților respective.

(2) Autoritatea de gestionare ia măsurile echivalente celor menționate la alineatul (1) referitoare la confidențialitate în ceea ce privește schimbul de informații suplimentare prin infrastructura de comunicare.

Articolul 18

Păstrarea înregistrărilor la nivel central

(1) Autoritatea de gestionare asigură că toate accesările și toate schimburile de date personale în cadrul CS-SIS sunt înregistrate în scopurile stipulate la articolul 12 alineatele (1) și (2).

(2) Înregistrările arată, în special, istoricul alertelor, data și ora transmisiei de date, datele folosite pentru efectuarea de căutări, o referință cu privire la datele transmise, precum și numele autorității competente responsabile de procesarea datelor.

(3) Înregistrările pot fi folosite doar în scopurile menționate la alineatul (1) și se șterg după cel puțin un an și cel mult trei ani de la creare. Înregistrările care includ istoricul alertelor pot fi șterse în termen de unu până la trei ani de la ștergerea alertelor.

(4) Înregistrările pot fi păstrate mai mult timp, dacă sunt necesare pentru procedurile de monitorizare care se află deja în curs de desfășurare.

(5) Autoritățile competente responsabile cu verificarea legalității căutărilor, monitorizarea legalității procesării datelor, automonitorizarea și asigurarea funcționării corespunzătoare a CS-SIS, precum și cu integritatea și securitatea datelor au acces la aceste înregistrări, în limitele competenței și la cerere, în scopul îndeplinirii obligațiilor ce le revin.

Articolul 19

Campania de informare

Comisia, în cooperare cu autoritățile naționale de control și cu Autoritatea Europeană pentru Protecția Datelor, organizează la începutul funcționării SIS II o campanie de informare care informează publicul cu privire la obiectivele, datele stocate, autoritățile care au acces și drepturile persoanelor. După înființarea sa, autoritatea de gestionare, în cooperare cu autoritățile naționale de control și cu Autoritatea Europeană pentru Protecția Datelor, organizează în mod repetat astfel de campanii. Statele membre, în cooperare cu propriile autorități naționale de control, concep și pun în aplicare politicile necesare de informare generală a cetățenilor lor cu privire la SIS II.

CAPITOLUL IV

CATEGORII DE DATE ȘI REPERE

Articolul 20

Categoriile de date

(1) Fără a aduce atingere articolului 8 alineatul (1) sau dispozițiilor prezentei decizii referitoare la stocarea datelor suplimentare, SIS II conține doar acele categorii de date care sunt furnizate de fiecare stat membru, după cum este necesar pentru scopurile prevăzute la articolele 26, 32, 34, 36 și 38.

(2) Categoriile de date sunt următoarele:

(a) persoanele în legătură cu care s-a emis o alertă;

(b) obiectele menționate la articolele 36 și 38.

(3) Informațiile despre persoanele în legătură cu care s-a emis o alertă se limitează la următoarele:

(a) nume și prenume, nume date la naștere și nume folosite anterior și orice alte pseudonime introduse separat;

(b) semnele fizice speciale, obiective și inalterabile;

(c) locul și data nașterii;

(d) sex;

(e) fotografii;

(f) amprente digitale;

(g) cetățenie (cetățenii);

(h) dacă persoanele respective sunt înarmate, violente sau au evadat;

(i) motivul alertei;

(j) autoritatea care emite alerta;

(k) o trimitere la deciziile care dau naștere unei alerte;

(l) măsurile ce trebuie luate;

(m) corelația/corelațiile cu alte alerte emise în SIS II conform articolului 52;

(n) tipul infracțiunii.

(4) Normele tehnice necesare pentru introducerea, actualizarea şi căutarea datelor prevăzute la alineatele (2) şi (3) se stabilesc în conformitate cu procedura menționată la articolul 67, fără a aduce atingere dispozițiilor instrumentului de constituire a autorității de gestionare.

(5) Normele tehnice necesare pentru căutarea datelor prevăzute la alineatul (3) sunt similare celor aplicabile în cazul căutărilor în CS-SIS, în copiile naționale şi în copiile tehnice, astfel cum se prevede la articolul 46 alineatul (2).

Articolul 21

Proporționalitatea

Înainte de a emite o alertă, statul membru stabileşte dacă respectivul caz este suficient de adecvat, relevant şi important pentru a se justifica introducerea sa în SIS II.

Articolul 22

Norme specifice pentru fotografii şi amprente digitale

Utilizarea fotografiilor şi a amprentelor digitale, astfel cum este prevăzut la articolul 20 alineatul (3) literele (e) şi (f), este supusă următoarelor dispoziții:

(a) fotografiile şi amprentele digitale se introduc doar în urma unei verificări speciale de calitate, pentru a se asigura îndeplinirea unui standard minim de calitate a datelor. Caracteristicile verificării speciale de calitate se stabilesc în conformitate cu procedura menționată la articolul 67, fără a aduce atingere dispozițiilor instrumentului de constituire a autorității de gestionare;

(b) fotografiile şi amprentele digitale se folosesc doar pentru confirmarea identității unei persoane care a fost localizată în urma unei căutări alfanumerice efectuate în SIS II;

(c) imediat ce devine posibil din punct de vedere tehnic, amprentele digitale pot fi folosite şi pentru identificarea unei persoane pe baza datelor sale biometrice de identificare. Înainte de introducerea acestei funcționalități în SIS II, Comisia prezintă un raport privind disponibilitatea şi gradul de adecvare al tehnologiei necesare, fiind consultat şi Parlamentul European.

Articolul 23

Cerințe referitoare la introducerea unei alerte

(1) Alertele cu privire la persoane nu pot fi introduse fără datele stipulate în articolul 20 alineatul (3) literele (a), (d), (l), precum şi, acolo unde este cazul, (k).

(2) Atunci când sunt disponibile, se introduc şi toate celelalte date enumerate la articolul 20 alineatul (3).

Articolul 24

Dispoziții generale privind reperele

(1) În cazul în care un stat membru consideră că faptul de a da curs unei alerte introduse în conformitate cu articolul 26, 32 sau 36 este incompatibil cu legislația sa internă, cu obligațiile sale internaționale sau cu interesele sale naționale vitale, statul membru respectiv poate solicita ulterior adăugarea unui reper la alertă, pentru ca acțiunea care se întreprinde în baza alertei să nu se desfăşoare pe teritoriul său. Reperul se adaugă de către biroul SIRENE al statului membru care a introdus alerta.

(2) Pentru a permite unui stat membru să solicite adăugarea unui reper la o alertă emisă în conformitate cu articolul 26, toate statele membre sunt notificate imediat cu privire la o nouă alertă din acea categorie prin schimb de informații suplimentare.

(3) Dacă în anumite cazuri urgente şi grave un stat membru care a emis o alertă solicită executarea acțiunii, statul membru care execută alerta examinează dacă este capabil să permită retragerea reperului adăugat la solicitarea sa urgentă. Dacă statul membru care execută alerta poate face acest lucru, va lua de îndată măsurile necesare pentru a asigura ca acțiunea ce se impune să fie îndeplinită imediat.

Articolul 25

Repere referitoare la alerte de arestare în vederea predării

(1) Atunci când se aplică Decizia-cadru 2002/584/JAI, reperul de împiedicare a arestării preventive se adaugă alertei de arestare în vederea predării, atunci când autoritatea judiciară competentă în baza legislației naționale să execute un mandat european de arestare a refuzat executarea acestuia în baza unui temei de neexecutare şi atunci când s-a solicitat adăugarea reperului.

(2) Cu toate acestea, la solicitarea urgentă a unei autorități judiciare competente în baza legislației naționale, fie în baza unor instrucțiuni de ordin general, fie într-un caz specific, se poate solicita adăugarea unui reper la o alertă de arestare în vederea predării, în cazul în care este evident că executarea mandatului european de arestare va trebui să fie refuzată.

CAPITOLUL V

ALERTELE PRIVIND PERSOANELE CĂUTATE PENTRU A FI ARESTATE ÎN VEDEREA PREDĂRII SAU A EXTRĂDĂRII

Articolul 26

Obiectivele şi condițiile de emitere a alertelor

(1) Datele privind persoanele căutate pentru a fi arestate în vederea predării în baza unui mandat european de arestare sau căutate pentru a fi arestate în vederea extrădării sunt introduse la cererea autorității judiciare a statului membru emitent.

(2) Datele privind persoanele căutate pentru a fi arestate în vederea predării se introduc pe baza mandatelor de arestare emise în conformitate cu acordurile încheiate între Uniunea Europeană şi ţările terţe în baza articolelor 24 şi 38 ale Tratatului UE în vederea predării persoanelor pe baza unui mandat de arestare, care prevăd transmiterea unui astfel de mandat de arestare prin intermediul Sistemului de informaţii Schengen.

Articolul 27

Date suplimentare referitoare la persoanele căutate pentru a fi arestate în vederea predării

(1) În cazul în care o persoană este căutată pentru a fi arestată în vederea predării în baza unui mandat european de arestare, statul emitent introduce în SIS II o copie a originalului mandatului european de arestare.

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

Articolul 28

Informaţii suplimentare referitoare la persoanele căutate pentru a fi arestate în vederea predării

Statul membru care a introdus în SIS II alerta de arestare în vederea predării comunică informaţiile menţionate la articolul 8 alineatul (1) din Decizia-cadru 2002/584/JAI tuturor statelor membre prin intermediul schimbului de informaţii suplimentare.

Articolul 29

Informaţii suplimentare referitoare la persoanele căutate pentru a fi arestate în vederea extrădării

(1) Statul membru care a introdus în SIS II alerta de arestare în vederea extrădării comunică tuturor statelor membre, prin intermediul schimbului de informaţii suplimentare, informaţiile următoare:

(a) autoritatea care a formulat cererea de arest;

(b) dacă există un mandat de arestare sau un alt document cu acelaşi efect juridic, sau o hotărâre executorie;

(c) natura şi încadrarea juridică a infracţiunii;

(d) o descriere a împrejurărilor în care s-a comis infracţiunea, inclusiv data, locul şi măsura în care persoana pentru care s-a emis alerta a participat la comiterea infracţiunii;

(e) în măsura în care este posibil, consecinţele infracţiunii;

(f) orice alte informaţii utile sau necesare pentru executarea alertei.

(2) Datele menţionate la alineatul (1) nu se comunică, dacă datele menţionate la articolul 27 sau 28 au fost deja furnizate şi sunt considerate suficiente pentru executarea alertei de către statul membru în cauză.

Articolul 30

Conversia alertelor privind persoanele căutate pentru a fi arestate în vederea predării sau a extrădării

Dacă arestarea nu se poate face, fie din cauza refuzului unui stat membru solicitat, exprimat în conformitate cu procedurile privind reperele stabilite la articolele 24 sau 25, fie deoarece investigaţia nu a fost finalizată în cazul unei alerte privind o arestare în vederea extrădării, statul membru solicitat trebuie să trateze alerta drept o alertă destinată comunicării locului unde se află persoana în cauză.

Articolul 31

Executarea unei acţiuni bazate pe o alertă cu privire la o persoană căutată pentru a fi arestată în vederea predării sau a extrădării

(1) O alertă introdusă în SIS II în conformitate cu articolul 26, în corelaţie cu datele suplimentare menţionate la articolul 27, constituie şi are acelaşi efect ca şi un mandat european de arestare eliberat în conformitate cu Decizia-cadru 2002/584/JAI, în cazurile în care se aplică respectiva decizie-cadru.

(2) În cazurile în care nu se aplică Decizia-cadru 2002/584/JAI, o alertă introdusă în SIS II în conformitate cu articolele 26 şi 29 produce aceleaşi efecte juridice ca o cerere de arestare provizorie în conformitate cu articolul 16 din Convenţia europeană privind extrădarea din 13 decembrie 1957 sau cu articolul 15 din Tratatul Benelux privind extrădarea şi asistenţa reciprocă judiciară în materie penală din 27 iunie 1962.

CAPITOLUL VI

ALERTELE PRIVIND PERSOANE DISPĂRUTE

Articolul 32

Obiectivele şi condiţiile de emitere a alertelor

(1) Datele privind persoanele dispărute care trebuie plasate sub protecţie şi/sau al căror loc trebuie determinat sunt introduse în SIS II la cererea autorităţii competente a statului membru care emite alerta.

(2) Se introduc următoarele categorii de persoane dispărute:

(a) persoane dispărute care trebuie plasate sub protecţie

(i) pentru propria lor protecţie;

(ii) pentru a preîntâmpina ameninţările;

(b) persoane dispărute care nu trebuie plasate sub protecţie.

(3) Alineatul (2) litera (a) se aplică numai persoanelor care trebuie reținute în temeiul unei hotărâri emise de o autoritate competentă.

(4) Alineatele (1), (2) și (3) se aplică în special minorilor.

(5) Statele membre garantează faptul că datele introduse în SIS II indică din ce categorie, dintre cele menționate la alineatul (2), face parte persoana dispărută.

Articolul 33

Executarea unei acțiuni bazate pe o alertă

(1) Autoritățile competente din locul unde se găsește o persoană din categoriile menționate la articolul 32 comunică statului membru care a emis alerta locul unde se află persoana respectivă, sub rezerva alineatului (2). În cazurile menționate la articolul 32 alineatul (2) litera (a), autoritățile competente pot să deplaseze persoana respectivă într-un loc sigur pentru a o împiedica să își continue călătoria, dacă legislația națională permite acest lucru.

(2) Orice comunicare, cu excepția celei dintre autoritățile competente, a datelor privind o persoană dispărută care a fost localizată și care este majoră se face numai cu consimțământul persoanei în cauză. Cu toate acestea, autoritățile competente pot comunica persoanei care a raportat dispariția faptul că alerta a fost ștearsă, deoarece persoana dispărută a fost localizată.

CAPITOLUL VII

ALERTELE PRIVIND PERSOANE CĂUTATE ÎN VEDEREA PARTICIPĂRII LA O PROCEDURĂ JUDICIARĂ

Articolul 34

Obiective și condiții de emitere a alertelor

Pentru a comunica reședința sau domiciliul, statele membre introduc în SIS II date privind următoarele aspecte, la cererea unei autorități competente:

(a) martori;

(b) persoanele care au primit citații de înfățișare în fața autorităților judecătorești în cadrul unei acțiuni penale pentru a răspunde în legătură cu fapte pentru care sunt acuzate;

(c) persoane cărora li se va comunica o hotărâre judecătorească sau alte documente privind o acțiune penală, pentru a răspunde în legătură cu fapte pentru care sunt acuzate;

(d) persoane cărora li se va prezenta o citație pentru a se prezenta în scopul ispășirii unei pedepse privative de libertate.

Articolul 35

Executarea acțiunii bazate pe o alertă

Informațiile solicitate sunt comunicate statului membru care le solicită prin intermediul schimbului de informații suplimentare.

CAPITOLUL VIII

ALERTELE PRIVIND PERSOANELE ŞI OBIECTELE CARE TREBUIE SĂ FACĂ OBIECTUL UNOR CONTROALE DISCRETE SAU SPECIFICE

Articolul 36

Obiective şi condiţii de emitere a alertelor

(1) Datele cu privire la persoane sau vehicule, ambarcațiuni, aeronave și containere se introduc în conformitate cu legislația națională a statului membru care emite alerta, în scopul unor controale discrete sau specifice, în conformitate cu articolul 37 alineatul (4).

(2) O astfel de alertă poate fi emisă în scopul urmăririi penale şi pentru prevenirea amenințărilor la adresa securității publice:

(a) în cazurile în care există o indicație clară potrivit căreia o persoană intenționează să comită sau comite o infracțiune gravă, precum infracțiunile menționate la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI; sau

(b) în cazul în care evaluarea generală a persoanei vizate, în special în temeiul infracțiunilor comise în trecut, generează suspiciunea că acea persoană va comite şi în viitor infracțiuni grave, precum cele menționate la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI.

(3) De asemenea, poate fi emisă o alertă în conformitate cu legislația internă, la cererea autorităților responsabile cu securitatea națională, dacă există dovezi clare că informațiile menționate la articolul 37 alineatul (1) sunt necesare pentru a preveni o amenințare serioasă din partea persoanei vizate sau amenințări serioase la adresa securității naționale interne sau externe. Statul membru care emite alerta în temeiul prezentului alineat informează celelalte state membre despre aceasta. Fiecare stat membru stabileşte căror autorități le vor fi transmise informațiile respective.

(4) Alertele privind vehiculele, ambarcațiunile, aeronavele şi containerele pot fi emise în cazul în care există dovezi clare că acestea au legătură cu infracțiunile grave menționate la alineatul (2) sau cu amenințările grave menționate la alineatul (3).

Articolul 37

Executarea acțiunii bazate pe o alertă

(1) În scopul unor controale discrete sau specifice, următoarele informații pot fi în totalitate sau parțial culese şi comunicate autorității care emite alerta, cu ocazia controalelor la frontieră sau a altor controale ale poliției şi a controalelor vamale în interiorul unui stat membru:

(a) faptul că s-a localizat persoana sau vehiculul, ambarcațiunea, aeronava sau containerul pentru care a fost emisă o alertă;

(b) locul, data sau motivul verificării;

(c) ruta şi destinaţia călătoriei;

(d) persoanele care însoţesc persoanele în cauză sau ocupanţii vehiculului, ai ambarcaţiunii, ai aeronavei, despre care se poate presupune pe baza unui temei raţional că sunt asociate cu persoanele în cauză;

(e) vehiculul, ambarcaţiunea, aeronava sau containerul;

(f) obiectele transportate;

(g) împrejurările în care s-a localizat persoana sau vehiculul, ambarcaţiunea, aeronava sau containerul.

(2) Informaţiile menţionate la alineatul (1) sunt comunicate prin intermediul schimbului de informaţii suplimentare.

(3) Pentru culegerea informaţiilor menţionate la alineatul (1), statele membre iau măsurile necesare pentru a nu periclita caracterul discret al verificării.

(4) În timpul controalelor specifice, vehiculele, ambarcaţiunile, aeronava, containerele şi obiectele transportate pot fi percheziţionate în conformitate cu legislaţia naţională din motivele menţionate la articolul 36. În cazul în care legislaţia unui stat membru interzice controalele specifice, acestea sunt înlocuite în mod automat, în statul membru respectiv, de controale discrete.

CAPITOLUL IX

ALERTELE PRIVIND OBIECTELE CĂUTATE PENTRU A FI CONFISCATE SAU FOLOSITE CA PROBE ÎN CURSUL PROCEDURILOR PENALE

Articolul 38

Obiective şi condiţii de emitere a alertelor

(1) Se introduc în SIS II datele cu privire la obiectele căutate pentru a fi confiscate sau folosite ca probe în cursul procedurilor penale.

(2) Se introduc următoarele categorii de obiecte uşor identificabile:

(a) autovehicule cu o capacitate cilindrică de peste 50 centimetri cubi, ambarcaţiuni şi aeronave;

(b) remorci cu un tonaj în vid de peste 750 kg, caravane, echipamente industriale, motoare exterioare şi containere;

(c) arme de foc;

(d) documente oficiale în alb care au fost furate, deturnate sau pierdute;

(e) documente de identitate eliberate, de tipul paşapoartelor, cărţilor de identitate, permiselor de conducere, permiselor de reşedinţă şi documentelor de călătorie furate, însuşite ilegal, pierdute sau anulate;

(f) certificate de înmatriculare ale vehiculelor sau plăci cu numărul de înmatriculare care au fost furate, deturnate, pierdute sau anulate;

(g) bancnote (bancnote înregistrate);

(h) valori mobiliare şi mijloace de plată, cum ar fi cecuri, cărţi de credit, obligaţiuni şi acţiuni, care au fost furate, însuşite ilegal, pierdute sau anulate.

(3) Normele tehnice necesare pentru introducerea, actualizarea, ştergerea şi căutarea datelor prevăzute la alineatul (2) se stabilesc în conformitate cu procedura menţionată la articolul 67, fără a aduce atingere dispoziţiilor instrumentului de constituire a autorităţii de gestionare.

Articolul 39

Executarea acţiunii bazate pe o alertă

(1) Dacă o operaţiune de căutare indică existenţa unei alerte în cazul unui obiect care a fost localizat, autoritatea care a coroborat cele două informaţii contactează autoritatea care a emis alerta pentru a se conveni măsurile care urmează să fie adoptate. În acest scop, se pot comunica şi date cu caracter personal, în conformitate cu prezenta decizie.

(2) Informaţiile menţionate la alineatul (1) sunt comunicate prin intermediul schimbului de informaţii suplimentare.

(3) Statul membru care a localizat obiectul ia măsuri în conformitate cu legislaţia naţională.

CAPITOLUL X

DREPTUL DE ACCES ŞI REŢINEREA ALERTELOR

Articolul 40

Autorităţile care au drept de acces la alerte

(1) Accesul la datele introduse în SIS II şi dreptul de a consulta astfel de date în mod direct sau într-o copie a datelor din SIS II sunt rezervate exclusiv autorităţilor responsabile cu:

(a) controlul de frontieră, în conformitate cu Regulamentul (CE) nr. 562/2006 al Parlamentului European şi al Consiliului din 15 martie 2006 de instituire a unui Cod Comunitar privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen) [1];

(b) alte controale efectuate de poliţie şi autorităţile vamale, desfăşurate în interiorul statului membru interesat, coordonarea acestora de către autorităţi desemnate.

(2) Cu toate acestea, dreptul de acces la datele introduse în SIS II şi dreptul de a consulta astfel de date în mod direct poate fi exercitat şi de autorităţi naţionale judiciare, inclusiv cele responsabile cu iniţierea urmăririi penale în acţiunile penale şi cu anchete judiciare anterioare punerii sub acuzare, în îndeplinirea sarcinilor lor, în conformitate cu legislaţia naţională, precum şi de către autorităţile lor coordonatoare.

[1] JO L 105, 13.4.2006, p. 1.

(3) Autoritățile menționate în cuprinsul prezentului articol sunt incluse pe lista menționată la articolul 46 alineatul (8).

Articolul 41

Accesul Europol la datele SIS II

(1) În temeiul mandatului său, Oficiul European de Poliție (Europol) are drept de acces şi consultare directă a datelor introduse în SIS II, în conformitate cu articolele 26, 36 şi 38.

(2) În cazul în care o consultare efectuată de Europol dezvăluie existența unei alerte în SIS II, Europol informează, prin intermediul canalelor definite de Convenția Europol, statul membru care a emis alerta.

(3) Utilizarea informațiilor obținute în urma consultării SIS II este condiționată de acordul statului membru în cauză. În cazul în care statul membru permite utilizarea informațiilor respective, prelucrarea acestora este reglementată de Convenția Europol. Europol poate comunica aceste informații unor țări şi organisme terțe numai cu acordul statului membru în cauză.

(4) Europol poate solicita statului membru implicat informații suplimentare în conformitate cu dispozițiile Convenției Europol.

(5) Europol:

(a) înregistrează toate accesările şi consultările de date pe care le efectuează, în conformitate cu dispozițiile articolului 12;

(b) fără a aduce atingere alineatelor (3) şi (4), nu conectează porțiuni din SIS II cu un alt computer şi nu transferă datele conținute în SIS II, în scopul colectării şi prelucrării datelor realizate de către sau la Europol, şi nu descarcă ori copiază în niciun alt mod vreo porțiune din SIS II;

(c) limitează accesul la datele introduse în SIS II la personalul Europol autorizat în mod explicit în acest sens;

(d) adoptă şi aplică măsurile prevăzute la articolele 10 şi 11;

(e) permite organismului de control comun, constituit în temeiul articolului 24 din Convenția Europol, să reexamineze activitățile întreprinse de Europol în cursul exercitării dreptului său de acces şi de consultare a datelor introduse în SIS II.

Articolul 42

Accesul Eurojust la datele SIS II

(1) În temeiul mandatului lor, membrii naționali ai Eurojust şi adjuncții acestora au drept de acces şi consultare directă a datelor introduse în SIS II, în conformitate cu articolele 26, 32, 34 şi 38.

(2) În cazul în care o consultare efectuată de un membru național al Eurojust dezvăluie existența unei alerte în SIS II, acesta informează în acest sens statul membru care a emis alerta. Orice comunicare a informațiilor obținute în urma unei astfel de consultări poate fi adresată unor țări şi organisme terțe numai cu acordul statului membru care a emis alerta.

(3) Niciun element din cuprinsul prezentului articol nu este interpretat ca o limitare a dispozițiilor Deciziei 2002/187/JAI privind protecția datelor şi responsabilitatea pentru prelucrarea neautorizată sau incorectă a acestor date de către membrii Eurojust sau adjuncții acestora sau ca o îngrădire a prerogativelor comitetului comun de control constituit în temeiul respectivei decizii.

(4) Orice accesare şi consultare efectuate de un membru național al Eurojust sau de un adjunct al acestuia este înregistrată în conformitate cu dispozițiile articolului 12, iar orice utilizare de către aceştia a datelor accesate este înregistrată.

(5) Porțiunile din SIS II la care au avut acces membrii naționali sau adjuncții acestora nu se conectează şi nu se transferă datele pe care le conțin către vreun sistem informatic în scopul colectării şi prelucrării datelor realizate de către sau la Eurojust, şi nici nu se descarcă vreo porțiune din SIS II.

(6) Accesul la datele introduse în SIS II este limitat la membrii naționali şi la adjuncții acestora şi nu este extins la personalul Eurojust.

(7) Se adoptă şi se aplică măsurile prevăzute la articolele 10 şi 11, destinate asigurării securității şi confidențialității.

Articolul 43

Limitele de acces

Utilizatorii, inclusiv Europol, membrii naționali ai Eurojust şi adjuncții acestora pot accesa numai datele care le sunt necesare în scopul îndeplinirii atribuțiilor ce le revin.

Articolul 44

Perioada de păstrare a alertelor privind persoanele

(1) Alertele privind persoanele introduse în SIS II în temeiul prezentei decizii sunt păstrate numai atât timp cât este necesar pentru realizarea scopurilor pentru care au fost introduse.

(2) Un stat membru care emite o alertă reexaminează nevoia de a o menține în termen de trei ani de la introducerea acesteia în SIS II. Perioada respectivă este de un an în cazul alertelor privind persoanele menționate la articolul 36.

(3) Fiecare stat membru stabileşte, după caz, perioade de reexaminare mai scurte, în conformitate cu legislația sa națională.

(4) În timpul perioadei de reexaminare, statul membru care emite alerta poate decide, în urma unei evaluări individuale cuprinzătoare care urmează a fi înregistrată, să mențină alerta, dacă acest lucru se dovedește necesar pentru scopul în care a fost emisă. În acest caz, alineatul (2) se aplică, de asemenea, și prelungirii. Orice prelungire a duratei unei alerte este comunicată către CS-SIS.

(5) Alertele sunt șterse automat după expirarea perioadei de reexaminare menționate la alineatul (2), cu excepția cazurilor în care statul membru care a emis alerta a informat CS-SIS cu privire la prelungirea alertei, în temeiul alineatului (4). CS-SIS informează automat statele membre asupra ștergerii programate a datelor din sistem, cu patru luni în avans.

(6) Statele membre realizează statistici privind numărul alertelor a căror perioadă de reținere a fost prelungită în conformitate cu alineatul (4).

Articolul 45

Perioada de păstrare a alertelor privind obiectele

(1) Alertele privind obiectele introduse în SIS II în temeiul prezentei decizii sunt păstrate numai atât timp cât este necesar pentru realizarea scopurilor pentru care au fost introduse.

(2) Alertele privind obiectele introduse în conformitate cu articolul 36 sunt păstrate maximum cinci ani.

(3) Alertele privind obiectele introduse în conformitate cu articolul 38 sunt păstrate maximum zece ani.

(4) Perioadele de păstrare menționate la alineatele (2) și (3) pot fi prelungite, dacă acest lucru se dovedește necesar pentru scopul în care a fost emisă alerta. În acest caz, alineatele (2) și (3) se aplică, de asemenea, și prelungirii.

CAPITOLUL XI

REGULI GENERALE DE PRELUCRARE A DATELOR

Articolul 46

Prelucrarea datelor din SIS II

(1) Statele membre pot prelucra datele menționate la articolele 20, 26, 32, 34, 36 și 38 numai în scopurile stabilite pentru fiecare categorie de alerte menționate la articolele respective.

(2) Datele pot fi copiate numai în scopuri tehnice, cu condiția ca această copiere să fie necesară pentru ca autoritățile menționate la articolul 40 să poată efectua o consultare directă. Dispozițiile prezentei decizii se aplică copiilor respective. Alertele emise de un stat membru nu pot fi copiate din sistemul său N.SIS II în alte fișiere de date naționale.

(3) Copiile tehnice menționate la alineatul (2) care conțin legături la baze de date offline pot fi păstrate maximum 48 de ore. Perioada poate fi prelungită, în caz de urgență, până la încetarea urgenței.

Statele membre realizează un inventar la zi al acestor copii, îl pun la dispoziția autorității lor naționale de supraveghere și asigură aplicarea în cazul copiilor respective a dispozițiilor deciziei în cauză, în special ale articolului 10.

(4) Accesul la date este autorizat numai în limita competenței autorităților naționale menționate la articolul 40 și numai pentru personalul autorizat în acest sens.

(5) Cu privire la alertele prevăzute la articolele 26, 32, 34, 36 și 38 ale prezentei decizii, orice prelucrare a informațiilor conținute în acestea în scopuri diferite de cele pentru care a fost introdusă alerta trebuie corelată cu un caz specific și trebuie să fie justificată de necesitatea de a preveni o amenințare gravă, iminentă la adresa ordinii și securității publice, de serioase temeiuri de securitate națională sau în scopul prevenirii unei infracțiuni grave. În acest scop, trebuie obținută o autorizare prealabilă din partea statului membru care a emis alerta.

(6) Datele nu pot fi utilizate în scopuri administrative.

(7) Orice utilizare a datelor care contravine dispozițiilor alineatelor (1)-(6) este considerată abuz în temeiul dreptului național al fiecărui stat membru.

(8) Fiecare stat membru înaintează autorității de gestionare o listă a autorităților competente care sunt autorizate să consulte direct datele conținute în SIS II în temeiul prezentei decizii, precum și orice modificări ale listei. Lista specifică, în cazul fiecărei autorități, ce date pot fi consultate și în ce scopuri. Autoritatea de gestionare asigură publicarea anuală a listei în *Jurnalul Oficial al Uniunii Europene*.

(9) În măsura în care Uniunea Europeană nu stabilește dispoziții specifice, legislația fiecărui stat membru se aplică datelor introduse în sistemul său N.SIS II.

Articolul 47

Datele SIS II și fișierele naționale

(1) Articolul 46 alineatul (2) nu aduce atingere dreptului unui stat membru de a stoca în fișierele sale naționale datele SIS II în legătură cu care s-au luat măsuri pe teritoriul său. Astfel de date sunt stocate în fișiere naționale maximum trei ani, cu excepția cazului în care dispoziții specifice din legislația națională prevăd o perioadă de păstrare mai îndelungată.

(2) Articolul 46 alineatul (2) nu aduce atingere dreptului unui stat membru de a stoca în fișiere naționale datele cuprinse într-o anumită alertă emisă în SIS II de către statul membru respectiv.

Articolul 48

Informații în cazul neexecutării alertelor

Dacă măsurile solicitate nu pot fi aplicate, statul membru solicitat informează de îndată statul membru care a emis alerta.

Articolul 49

Calitatea datelor procesate în SIS II

(1) Un stat membru care emite o alertă are responsabilitatea de a asigura precizia şi actualitatea datelor introduse în SIS II, precum şi caracterul legal al introducerii acestora.

(2) Numai statul membru care a emis alerta este autorizat să modifice, să suplimenteze, să corecteze, să actualizeze sau să şteargă datele pe care le-a introdus.

(3) Dacă un stat membru, altul decât cel care a emis alerta, deține dovezi care indică faptul că una dintre date este incorectă sau a fost stocată ilegal, acesta informează în acest sens, prin schimbul de informații suplimentare, statul membru care a emis alerta, cu prima ocazie şi nu mai târziu de zece zile de la data la care i-au fost aduse la cunoştință dovezile respective. Statul membru care a emis alerta verifică comunicarea şi, dacă este necesar, corectează sau şterge imediat datele respective.

(4) În cazul în care statele membre nu reuşesc să ajungă la un acord în termen de două luni, statul membru care nu a emis alerta prezintă situația Autorității Europene pentru Protecția Datelor, care acționează ca mediator, de comun acord cu autoritățile de supraveghere interesate.

(5) Statele membre fac schimb de informații suplimentare în cazul în care o persoană depune o reclamație prin care afirmă că nu este persoana căutată printr-o alertă. Dacă rezultatul controlului arată că, de fapt, este vorba de două persoane diferite, reclamantul este informat asupra dispozițiilor articolului 51.

(6) Dacă o persoană face deja obiectul unei alerte în SIS II, statul membru care introduce o nouă alertă ajunge la un acord cu privire la introducerea alertei cu statul membru care a introdus prima alertă. Acordul se obține în urma schimbului de informații suplimentare.

Articolul 50

Diferențierea persoanelor cu caracteristici similare

În cazul în care se constată, în momentul introducerii unei noi alerte, că există deja în SIS II o persoană având acelaşi element descriptiv al identității, este urmată următoarea procedură:

(a) biroul SIRENE contactează autoritatea solicitantă, pentru a clarifica dacă alerta se referă la aceeaşi persoană;

(b) în cazul în care verificarea coroborată arată că subiectul noii alerte şi persoana prezentă deja în SIS sunt identice, biroul SIRENE aplică procedura de introducere a alertelor multiple menționată la articolul 49 alineatul (6). În cazul în care rezultatul verificării arată că, de fapt, este vorba de două persoane diferite, biroul SIRENE aprobă cererea de a introduce o a doua alertă, adăugând elementele necesare pentru a evita orice identificare eronată.

Articolul 51

Date suplimentare pentru tratarea identităților de care s-a abuzat

(1) În cazul în care pot apărea confuzii între persoana care trebuia să constituie subiectul unei alerte şi o persoană de a cărei identitate s-a abuzat, statul membru care a introdus alerta adaugă date privitoare la cea de-a doua persoană, pentru a evita consecințele negative ale identificării eronate.

(2) Datele privind o persoană de a cărei identitate s-a abuzat sunt folosite doar în următoarele scopuri:

(a) pentru a permite autorității competente să distingă între persoana de a cărei identitate s-a abuzat şi persoana care a făcut, de fapt, obiectul alertei;

(b) pentru a permite persoanei de a cărei identitate s-a abuzat să îşi dovedească identitatea şi să confirme faptul că s-a abuzat de identitatea sa.

(3) În sensul prezentului articol, pot fi introduse şi procesate ulterior în cadrul SIS II exclusiv următoarele date cu caracter personal:

(a) nume şi prenume, nume date la naştere şi nume folosite anterior, şi orice alte pseudonime introduse separat;

(b) orice semne fizice speciale, obiective şi inalterabile;

(c) locul şi data naşterii;

(d) sex;

(e) fotografii;

(f) amprente digitale;

(g) cetățenie (cetățenii);

(h) numărul documentelor de identitate şi data emiterii acestora.

(4) Normele tehnice necesare pentru introducerea şi procesarea ulterioară a datelor prevăzute la alineatul (3) se stabilesc în conformitate cu procedura menționată la articolul 67, fără a aduce atingere dispozițiilor instrumentului de constituire a autorității de gestionare.

(5) Datele menționate la alineatul (3) sunt eliminate concomitent cu alerta respectivă sau mai devreme, dacă persoana solicită acest lucru.

(6) Datele menționate la alineatul (3) pot fi accesate exclusiv de autoritățile care au drept de acces la alerta respectivă. Acestea au acces doar în scopul evitării unei identificări eronate.

Articolul 52

Conexiuni între alerte

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

(2) Crearea unei conexiuni nu afectează acțiunea specifică ce urmează a fi întreprinsă în baza alertelor conectate sau perioada de stocare a alertelor conectate.

(3) Crearea unei conexiuni nu afectează drepturile de acces prevăzute de prezenta directivă. Autoritățile care nu au drept de acces la anumite categorii de alerte nu pot vedea conexiunea la o alertă la care nu au acces.

(4) Un stat membru creează o conexiune între alerte doar în cazul în care există o necesitate operațională clară.

(5) Un stat membru poate crea conexiuni în conformitate cu legislația sa internă, cu condiția să respecte principiile prezentate în prezentul articol.

(6) În cazul în care un stat membru consideră că crearea de către un alt stat membru a unei conexiuni între alerte este incompatibilă cu legislația sa internă sau cu obligațiile sale internaționale, statul membru respectiv poate lua măsurile necesare pentru a se asigura că această conexiune nu poate fi accesată de pe teritoriul său sau de către autoritățile sale situate în afara teritoriului său.

(7) Procedurile tehnice pentru conectarea alertelor se stabilesc în conformitate cu procedura menționată la articolul 67, fără a aduce atingere dispozițiilor instrumentului de constituire a autorității de gestionare.

Articolul 53

Scopul şi perioada de stocare a informațiilor suplimentare

(1) Statele membre păstrează o trimitere la deciziile care dau naştere unei alerte la biroul SIRENE pentru sprijinirea schimbului de informații suplimentare.

(2) Datele cu caracter personal păstrate în fişiere de biroul SIRENE în urma unui schimb de informații sunt stocate doar pe parcursul unei perioade de timp necesare pentru îndeplinirea obiectivelor pentru care acestea au fost furnizate. În orice caz, acestea sunt şterse în decurs de maximum un an după ce alerta respectivă a fost ştearsă din SIS II.

(3) Alineatul (2) nu aduce atingere dreptului unui stat membru de a stoca în fişiere naționale informații privitoare la o anumită alertă pe care a emis-o statul membru respectiv sau la o alertă în legătură cu care s-au luat măsuri pe teritoriul său. Perioada în care astfel de date pot fi păstrate în fişiere naționale este reglementată de legislația internă.

Articolul 54

Transferul datelor cu caracter personal către terți

Datele prelucrate în cadrul SIS II în temeiul prezentei decizii nu trebuie transferate sau puse la dispoziția țărilor terțe sau a organizațiilor internaționale.

Articolul 55

Schimbul de date cu Interpol privind paşapoartele furate, însuşite ilegal, pierdute sau anulate

(1) Prin derogare de la articolul 54, se poate face schimb de informații cu membrii Interpol în ceea ce priveşte numărul paşaportului, țara emitentă şi tipul de document al paşapoartelor furate, însuşite ilegal, pierdute sau anulate, introduse în SIS II, prin stabilirea unei conexiuni între SIS II şi baza de date Interpol care cuprinde documente de călătorie furate sau pierdute, sub rezerva concluziei la care se ajunge în cadrul unui acord între Interpol şi Uniunea Europeană. Acordul prevede ca transmiterea datelor introduse de un stat membru să se afle sub rezerva consimțământului statului respectiv.

(2) Acordul menționat la alineatul (1) prevede ca schimbul de date să fie accesibil exclusiv membrilor Interpol din țările care garantează un grad de protecție adecvat al datelor cu caracter personal. Înainte de încheierea acestui acord, Consiliul solicită avizul Comisiei cu privire la compatibilitatea nivelului de protecție a datelor cu caracter personal şi respectarea drepturilor şi libertăților fundamentale privind procesarea automată a datelor cu caracter personal de către Interpol şi țările care au membri delegați la Interpol.

(3) Acordul menționat la alineatul (1) poate prevedea, de asemenea, accesul statelor membre prin intermediul SIS II la datele din baza de date Interpol care cuprinde documente de călătorie furate sau pierdute, în conformitate cu dispozițiile relevante ale prezentei decizii care reglementează alertele cu privire la paşapoartele furate, însuşite ilegal, pierdute sau anulate şi introduse în SIS II.

CAPITOLUL XII

PROTECȚIA DATELOR

Articolul 56

Procesarea categoriilor de date sensibile

Procesarea categoriilor de date enumerate la prima teză a articolului 6 din Convenția Consiliului Europei pentru protecția persoanelor în legătură cu prelucrarea automată a datelor cu caracter personal din 28 ianuarie 1981 nu este autorizată.

Articolul 57

Aplicarea Convenției Consiliului Europei privind protecția datelor

Datele cu caracter personal procesate în temeiul prezentei decizii sunt protejate în conformitate cu Convenția Consiliului Europei din 28 ianuarie 1981 pentru protecția persoanelor în legătură cu prelucrarea automată a datelor cu caracter personal, şi cu orice modificări ulterioare ale acesteia.

Articolul 58

Dreptul de acces, rectificarea datelor incorecte şi eliminarea datelor stocate în mod ilegal

(1) Dreptul persoanelor de a avea acces la datele introduse în SIS II care le privesc, în conformitate cu prezenta decizie, se exercită în conformitate cu legislația statului membru față de care ele invocă acest drept.

(2) În cazul în care legislația internă prevede acest lucru, autoritatea națională de control decide dacă informațiile se pot comunica şi prin ce modalitate.

(3) Un alt stat membru decât cel care a emis o alertă poate comunica informații privind astfel de date numai dacă a oferit în prealabil ocazia statului membru care a emis alerta să-şi facă cunoscută poziția. Acest lucru se realizează prin intermediul unui schimb de informații suplimentare.

(4) Informațiile nu sunt comunicate persoanei care face obiectul acestor date, dacă acest lucru este indispensabil pentru efectuarea unei operații legale în legătură cu alerta sau pentru apărarea drepturilor şi libertăților unor terțe părți.

(5) Orice persoană are dreptul de a obține rectificarea datelor care o privesc care conțin erori de fapt sau eliminarea datelor care o privesc care sunt stocate ilegal.

(6) Persoana interesată este informată cât mai curând posibil şi, în orice caz, într-un termen de maximum 60 de zile de la data la care depune cererea de acces sau mai devreme, în cazul în care acest lucru este prevăzut de legislația națională.

(7) Persoana interesată este informată cu privire la rezultatul exercitării drepturilor acesteia de rectificare şi eliminare cât mai curând posibil şi, în orice caz, într-un termen care nu depăşeşte trei luni de la data la care a depus cererea de rectificare sau de eliminare sau mai devreme, în cazul în care acest lucru este prevăzut de legislația națională.

Articolul 59

Căi de atac

(1) Orice persoană poate introduce o acțiune la instanțele judecătoreşti sau la autoritatea competentă conform legislației naționale a oricărui stat membru pentru accesarea, rectificarea, eliminarea sau obținerea de informații sau pentru obținerea de compensații în legătură cu o alertă care o priveşte.

(2) Statele membre se angajează reciproc să aplice deciziile definitive pronunțate de instanțele judecătoreşti sau de autoritățile menționate la alineatul (1), fără a aduce atingere dispozițiilor articolului 64.

(3) Normele privind căile de atac prevăzute în prezentul articol sunt evaluate de Comisie până la 23 august 2009.

Articolul 60

Supravegherea sistemului N.SIS II

(1) Fiecare stat membru se asigură că o autoritate independentă („autoritatea națională de control") monitorizează independent legalitatea prelucrării datelor cu caracter personal din cadrul SIS II pe teritoriul lor şi transmiterea acestora de pe teritoriul lor, precum şi schimbul şi procesarea ulterioară a informațiilor suplimentare.

(2) Autoritatea națională de control se asigură că auditarea operațiunilor de prelucrare a datelor în cadrul N.SIS II se efectuează în conformitate cu standardele internaționale de audit cel puțin o dată la patru ani.

(3) Statele membre garantează că autoritatea națională de control are la dispoziție resurse suficiente pentru a-şi îndeplini sarcinile care i-au fost încredințate în temeiul prezentei decizii.

Articolul 61

Supravegherea autorității de gestionare

(1) Autoritatea Europeană pentru Protecția Datelor verifică dacă activitățile de prelucrare a datelor cu caracter personal desfăşurate de autoritatea de gestionare sunt efectuate în conformitate cu prezenta decizie. Îndatoririle şi competențele prevăzute la articolele 46 şi 47 din Regulamentul (CE) nr. 45/2001 se aplică în mod corespunzător.

(2) Autoritatea Europeană pentru Protecția Datelor se asigură că auditarea activităților de prelucrare a datelor cu caracter personal desfăşurate de autoritatea de gestionare este efectuată în conformitate cu standardele internaționale de audit cel puțin o dată la patru ani. Un raport privind un asemenea audit se transmite Parlamentului European, Consiliului, autorității de gestionare, Comisiei şi autorităților naționale de control. Autorității de gestionare i se oferă posibilitatea de a formula observații înainte ca raportul să fie adoptat.

Articolul 62

Cooperarea între autoritățile naționale de control şi Autoritatea Europeană pentru Protecția Datelor

(1) Autoritățile naționale de control şi Autoritatea Europeană pentru Protecția Datelor, acționând fiecare în limitele competențelor proprii, cooperează în mod activ în cadrul responsabilităților lor şi asigură supravegherea coordonată a SIS II.

(2) Acestea, acționând fiecare în limitele competențelor lor respective, fac schimb de informații relevante, se asistă reciproc în efectuarea auditurilor şi controalelor, examinează dificultățile de interpretare sau de aplicare a prezentei decizii, studiază problemele care pot apărea în timpul exercitării activităților de supraveghere independentă sau în timpul exercitării drepturilor persoanelor care fac obiectul acestor date, elaborează propuneri armonizate pentru identificarea de soluții comune la problemele existente şi promovează conştientizarea drepturilor legate de protecția datelor, după caz.

(3) Autoritățile naționale de control şi Autoritatea Europeană pentru Protecția Datelor se reunesc în acest scop cel puțin de două ori pe an. Autoritatea Europeană pentru Protecția Datelor suportă costurile şi asigură serviciile aferente acestor reuniuni. Regulamentul de procedură se adoptă în cadrul primei reuniuni. Alte metode de lucru se stabilesc de comun acord, după caz. Un raport comun de activitate se transmite Parlamentului European, Consiliului, Comisiei şi autorității de gestionare o dată la doi ani.

Articolul 63

Protecția datelor în perioada de tranziție

În cazul în care Comisia îşi delegă responsabilitățile în cursul perioadei de tranziție către un alt organism sau către alte organisme, în temeiul articolului 15 alineatul (4), aceasta se asigură că Autoritatea Europeană pentru Protecția Datelor are dreptul şi este capabilă să îşi exercite pe deplin sarcinile, inclusiv efectuarea de controale la fața locului, şi să îşi exercite orice alte competențe care i-au fost conferite în temeiul articolului 47 din Regulamentul (CE) nr. 45/2001.

CAPITOLUL XIII

RĂSPUNDEREA ŞI SANCȚIUNI

Articolul 64

Răspunderea

(1) Fiecare stat membru răspunde, în conformitate cu legislația sa internă, pentru orice prejudiciu cauzat unei persoane ca urmare a utilizării sistemului N.SIS II. Aceasta se aplică şi prejudiciului cauzat de statul membru care a emis alerta, dacă acesta a introdus efectiv date incorecte sau a stocat date în mod ilegal.

(2) Dacă statul membru împotriva căruia se introduce o acțiune nu este statul membru care emite alerta, acesta din urmă trebuie să ramburseze, la cerere, sumele plătite drept compensație, cu excepția cazului în care utilizarea datelor de către statul membru care solicita rambursarea încalcă prezenta decizie.

(3) Dacă nerespectarea de către un stat membru a obligațiilor care îi revin în temeiul prezentei decizii provoacă daune sistemului SIS II, statul membru respectiv răspunde pentru aceste daune, cu excepția cazului şi în măsura în care autoritatea de gestionare sau un alt stat membru care participă la SIS II nu a luat măsurile necesare pentru a preveni provocarea daunelor sau pentru a le reduce impactul.

Articolul 65

Sancțiuni

Statele membre se asigură că orice utilizare frauduloasă a datelor introduse în SIS II sau orice schimb de informații suplimentare care contravin prezentei decizii se află sub rezerva unor sancțiuni eficiente, proporționale şi disuasive în conformitate cu legislația internă.

CAPITOLUL XIV

DISPOZIȚII FINALE

Articolul 66

Monitorizarea şi statisticile

(1) Autoritatea de gestionare se asigură că sunt aplicate proceduri pentru monitorizarea funcționării sistemului SIS II în raport cu obiectivele stabilite, în privința producției, a raportului cost-eficiență, a securității şi a calității serviciului.

(2) În scopul întreținerii tehnice, al raportării şi al realizării statisticilor, autoritatea de gestionare are acces la informațiile necesare cu privire la operațiunile de prelucrare efectuate în cadrul SIS II central.

(3) Autoritatea de gestionare publică în fiecare an statisticile care arată numărul de înregistrări pe categorii de alerte, numărul de rezultate pe categorii de alerte şi de câte ori a fost accesat SIS II, în total şi pe fiecare stat membru.

(4) La doi ani de la punerea în funcțiune a SIS II şi, ulterior, o dată la doi ani, autoritatea de gestionare prezintă Parlamentului European şi Consiliului un raport privind funcționarea SIS II central şi a infrastructurii de comunicare, inclusiv securitatea acestuia, şi schimbul bilateral şi multilateral de informații suplimentare dintre statele membre.

(5) La trei ani de la punerea în funcțiune a SIS II şi, ulterior, o dată la patru ani, Comisia prezintă o evaluare generală a SIS II central şi a schimbului bilateral şi multilateral de informații suplimentare dintre statele membre. Această evaluare generală include o examinare a rezultatelor obținute în comparație cu obiectivele şi o evaluare a consecvenței valabilității raționamentului care stă la baza prezentei decizii, a aplicării prezentei decizii cu privire la SIS II central, a securității SIS II central, precum şi a eventualelor implicații ale operațiunilor viitoare. Comisia transmite această evaluare Parlamentului European şi Consiliului.

(6) Statele membre pun la dispoziția autorității de gestionare și a Comisiei informațiile necesare pentru întocmirea rapoartelor menționate la alineatele (3), (4) și (5).

(7) Autoritatea de gestionare pune la dispoziția Comisiei informațiile necesare pentru întocmirea evaluărilor generale menționate la alineatul (5).

Articolul 67

Comitetul de reglementare

(1) În cazul în care se face trimitere la prezentul articol, Comisia este asistată de un comitet de reglementare format din reprezentanții statelor membre și prezidat de reprezentantul Comisiei. Reprezentantul Comisiei prezintă comitetului un proiect cu măsurile ce urmează a fi adoptate. Comitetul își dă avizul privind proiectul de măsuri într-un termen pe care președintele îl poate stabili în funcție de urgența problemei. Avizul se emite cu majoritatea prevăzută la articolul 205 alineatul (2) din Tratatul CE, în cazul deciziilor pe care Consiliul este chemat să le adopte în urma unei propuneri venite din partea Comisiei. Voturile reprezentanților statelor membre din cadrul comitetului sunt ponderate conform articolului menționat anterior. Președintele nu participă la vot.

(2) Comitetul își adoptă regulamentul de procedură în urma unei propuneri făcute de președinte pe baza normelor standard de procedură publicate în *Jurnalul Oficial al Uniunii Europene*.

(3) Comisia adoptă măsurile prevăzute, în cazul în care acestea sunt în conformitate cu avizul comitetului. În cazul în care măsurile prevăzute nu sunt în conformitate cu avizul comitetului sau dacă nu se emite un aviz, Comisia înaintează fără întârziere Consiliului o propunere privind măsurile ce urmează a fi luate.

(4) Consiliul poate hotărî cu majoritate calificată cu privire la propunere în termen de două luni de la prezentarea acesteia. În cazul în care, în acest termen, Consiliul s-a exprimat cu majoritate calificată că se opune propunerii, Comisia o reexaminează. Comisia poate prezenta Consiliului o propunere modificată, poate prezenta propunerea din nou sau poate prezenta o propunere legislativă. În cazul în care, la expirarea acestui termen, Consiliul nu adoptă măsurile de aplicare propuse și nici nu și-a exprimat opoziția față de propunerea măsurilor de aplicare, acestea sunt adoptate de către Comisie.

(5) Comitetul menționat la alineatul (1) își exercită funcția începând cu 23 august 2007.

Articolul 68

Modificarea dispozițiilor acquis-ului Schengen

(1) În sensul chestiunilor care intră în domeniul de aplicare al Tratatului privind Uniunea Europeană, prezenta decizie înlocuiește, la data menționată la articolul 71 alineatul (2), dispozițiile articolelor 64 și 92-119 din Convenția Schengen, cu excepția articolului 102 A.

(2) În sensul aspectelor care intră în domeniul de aplicare al Tratatului privind Uniunea Europeană, prezenta decizie înlocuiește, la data menționată la articolul 71 alineatul (2), următoarele dispoziții ale acquis-ului Schengen care pun în aplicare articolele respective [1]:

(a) Decizia Comitetului Executiv din 14 decembrie 1993 referitoare la regulamentul financiar privind costurile de instalare și de exploatare a Sistemului de informații Schengen (C.SIS) [SCH/Com-ex (93) 16];

(b) Decizia Comitetului Executiv din 7 octombrie 1997 privind dezvoltarea SIS [SCH/Com-ex (97) 24];

(c) Decizia Comitetului Executiv din 15 decembrie 1997 de modificare a Regulamentului Financiar privind C.SIS [SCH/Com-ex (97) 35];

(d) Decizia Comitetului Executiv din 21 aprilie 1998 privind C.SIS cu 15/18 conexiuni [SCH/Com-ex (98) 11];

(e) Decizia Comitetului Executiv din 25 aprilie 1997 privind adjudecarea contractului pentru studiul preliminar SIS II [SCH/Com-ex (97) 2 rev. 2];

(f) Decizia Comitetului Executiv din 28 aprilie 1999 privind costurile de instalare a C.SIS [SCH/Com-ex (99) 4];

(g) Decizia Comitetului Executiv din 28 aprilie 1999 privind adoptarea Manualului SIRENE [SCH/Com-ex (99) 5];

(h) Declarația Comitetului Executiv din 18 aprilie 1996 de definire a noțiunii de străin [SCH/Com-ex (96) decl. 5];

(i) Declarația Comitetului Executiv din 28 aprilie 1999 privind structura SIS [SCH/Com-ex (99) decl. 2 rev];

(j) Decizia Comitetului Executiv din 7 octombrie 1997 privind contribuțiile Norvegiei și ale Islandei la costurile de instalare și de exploatare a C.SIS [SCH/Com-ex (97) 18].

(3) În sensul chestiunilor care intră în domeniul de aplicare al Tratatului privind Uniunea Europeană, trimiterile la articolele înlocuite din Convenția Schengen și dispozițiile respective ale acquis-ului Schengen care pun în aplicare articolele sunt interpretate ca trimiteri la prezenta decizie.

Articolul 69

Abrogarea

Decizia 2004/201/JAI, Decizia 2005/211/JAI, Decizia 2005/719/JAI, Decizia 2005/727/JAI, Decizia 2006/228/JAI, Decizia 2006/229/JAI și Decizia 2006/631/JAI se abrogă de la data menționată la articolul 71 alineatul (2).

[1] JO L 239, 22.9.2000, p. 439.

Articolul 70

Perioada de tranziție și bugetul

(1) Alertele sunt transferate din SIS 1+ către SIS II. Statele membre asigură că, acordând prioritate alertelor privind persoanele, conținutul alertelor care sunt transferate din SIS 1+ în SIS II respectă dispozițiile prezentei decizii cât mai curând posibil și în termen de trei ani de la data menționată la articolul 71 alineatul (2). În cursul acestei perioade de tranziție, statele membre pot continua aplicarea dispozițiilor articolelor 94, 95 și 97-100 din Convenția Schengen la conținutul alertelor care sunt transferate din SIS 1+ în SIS II, sub rezerva următoarelor norme:

(a) în cazul unei modificări, adăugări, rectificări sau actualizări a conținutului unei alerte transferate din SIS 1+ în SIS II, statele membre se asigură că alerta respectă dispozițiile prezentei decizii începând de la data modificării, adăugirii, rectificării sau actualizării respective;

(b) în cazul unui rezultat la o alertă transferată din SIS 1+ în SIS II, statele membre examinează imediat compatibilitatea dintre alerta respectivă și dispozițiile prezentei decizii, însă fără a întârzia acțiunea care urmează să fie întreprinsă în baza alertei respective.

(2) Restul de buget la data stabilită în conformitate cu articolul 71 alineatul (2), care a fost aprobat în conformitate cu dispozițiile articolului 119 din Convenția Schengen, este restituit statelor membre. Sumele care urmează să fie restituite se calculează pe baza contribuțiilor din partea statelor membre în conformitate cu Decizia Comitetului executiv din 14 decembrie 1993 referitoare la regulamentul financiar privind costurile de instalare și de exploatare a Sistemului de informații Schengen.

(3) În timpul perioadei de tranziție menționate la articolul 15 alineatul (4), trimiterile din prezenta decizie la autoritatea de gestionare sunt interpretate ca trimiteri la Comisie.

Articolul 71

Intrarea în vigoare, aplicabilitatea și migrarea

(1) Prezenta decizie intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

(2) Se aplică statelor membre care participă la SIS 1+ începând cu datele care urmează să fie stabilite de Consiliu, hotărând prin unanimitatea membrilor săi, reprezentanți ai guvernelor statelor membre participante la SIS 1+.

(3) Datele menționate la alineatul (2) urmează să fie stabilite după ce:

(a) măsurile necesare de punere în aplicare au fost adoptate;

(b) fiecare stat membru participant la SIS 1+ aduce la cunoștința Comisiei faptul că a luat măsurile de ordin tehnic și juridic necesare prelucrării datelor din cadrul SIS II și schimbului de informații suplimentare;

(c) Comisia declară încheierea cu succes a unui test complet al SIS II, care este efectuat de Comisie împreună cu statele membre, iar grupurile pregătitoare ale Consiliului validează rezultatele propuse ale testului și confirmă că nivelul de performanță al SIS II este cel puțin echivalent cu cel îndeplinit de SIS 1+;

(d) Comisia a luat măsurile de ordin tehnic necesare conectării SIS II central la N.SIS II pentru statele membre implicate.

(4) Comisia aduce la cunoștința Parlamentului European rezultatele testului efectuat în conformitate cu prevederile alineatului (3) litera (c).

(5) Orice decizie adoptată de Consiliu în conformitate cu alineatul (2) se publică în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Luxemburg, 12 iunie 2007.

Pentru Consiliu
Președintele
F. TEIXEIRA DOS SANTOS