SISTEMUL DE INFORMAŢII SCHENGEN
GHID PENTRU EXERCITAREA DREPTULUI DE ACCES

I. INTRODUCERE SISTEMUL DE INFORMAŢII SCHENGEN GENERAŢIA A II-A (SIS II)

SIS II este un sistem IT la scară largă înfiinţat ca o măsură compensatorie pentru eliminarea controalelor la frontierele interne şi intenţionează să asigure un nivel ridicat de securitate în zona de libertate, securitate şi justiţie a Uniunii Europene, inclusiv menţinerea securităţii publice şi ordinii publice şi garantarea securităţii pe teritoriile statelor membre. SIS II este implementat deja în toate statele membre, cu excepţia Ciprului, Croaţiei şi Irlandei, precum şi în patru state asociate: Islanda, Norvegia, Elveţia şi Liechtenstein.
SIS II este un sistem de informaţii care permite autorităţilor naţionale de aplicare a legii, judiciare şi administrative să îndeplinească atribuţii specifice prin schimbul de date relevante. Agenţiile Europene EUROPOL şi EUROJUST au acces limitat la acest sistem.

Categorii de informaţii prelucrate

SIS II centralizează două mari categorii de informaţii ce iau forma alertelor privind, în primul rând *persoane* – care sunt căutate pentru a fi arestate, au fost date dispărute, în vederea participării la o procedură judiciară, fac obiectul unor controale discrete sau specifice sau având interdicţie de şedere în spaţiul Schengen şi, în al doilea rând, *obiecte* – precum vehicule, documente de călătorie, cărţi de credit pentru a fi confiscate sau folosite ca probe în cursul procedurilor penale sau fac obiectul unor controale discrete sau specifice.

Temeiul legal

În funcţie de tipul de alertă, SIS II este reglementat de Regulamentul (CE) 1987/2006 al Parlamentului European şi al Consiliului din 20 decembrie 2006 privind instituirea, funcţionarea şi utilizarea Sistemului de Informaţii Schengen din a doua generaţie (SIS II) cu privire la procedurile pentru alerte ce intră sub incidenţa Titlului IV din Tratatul de înfiinţare a Comunităţii Europene (fostul pilon I) sau de Decizia Consiliului 2007/533/JAI a Consiliului din 12 iunie 2007 privind înfiinţarea, funcţionarea şi utilizarea Sistemului de informaţii Schengen de a doua generaţie în ceea ce priveşte procedurile ce intră sub incidenţa Titlului VI din Tratatul Uniunii Europene (fostul pilon III).

Categoriile de date personale prelucrate

Atunci când alerta se referă la o persoană, informaţiile trebuie să includă întotdeauna numele, prenumele şi orice pseudonim, sexul, o trimitere la decizia privind alerta şi acţiunea ce trebuie să

fie luată. Dacă sunt disponibile, alerta poate conţine informaţii precum orice caracteristici specifice, obiective sau fizice ce nu pot fi schimbate; locul şi data naşterii; fotografii; amprentele digitale; cetăţenia (cetăţeniile); dacă persoana în cauză este înarmată, violentă sau evadată; motivul alertei; autoritatea care emite alerta; legături cu alte alerte emise în SIS II în conformitate cu art. 37 din SIS II Regulamentul SIS II sau art. 52 din Decizia SIS II.

Arhitectura sistemului

SIS II este compus din:

- un sistem central („SIS II Central") ;
- un sistem naţional („N.SIS II") în fiecare dintre Statele Membre (sistemele naţionale de date care vor comunica cu SIS II Central);
- o infrastructură de comunicare între sistemul central şi sistemele naţionale care asigură o reţea virtuală criptată consacrată datelor SIS II şi schimbului de date între autorităţile responsabile pentru schimbul de informaţii suplimentare (Birourile SIRENE).

II. DREPTURILE PERSOANELOR ALE CĂROR DATE SUNT PRELUCRARE ÎN SIS II

În conformitate cu principiile protecţiei datelor, tuturor persoanelor ale căror date sunt prelucrare în SIS II le sunt recunoscute drepturile specifice prin Decizia SIS II şi Regulamentul SIS II menţionate mai sus.
Acestea sunt în principal:

- dreptul de acces la datele stocate în SIS II;
- dreptul de rectificare a datelor inexacte şi ştergerea datelor stocate în mod ilegal;
- dreptul de a introduce o acţiune la instanţele judecătoreşti sau la autoritatea competentă privind rectificarea sau ştergerea datelor sau pentru obţinerea de compensaţii.

Oricine persoană ce îşi exercită oricare dintre aceste drepturi se poate adresa autorităţilor competente din statul Schengen, la alegerea sa. Această opţiune este posibilă, deoarece toate bazele de date naţionale (N.SIS II) sunt identice cu baza de date centrală (CS.SIS). Prin urmare aceste drepturi pot fi exercitate în orice stat Schengen indiferent de statul care a emis alerta.
Atunci când o persoană îşi exercită dreptul de acces, de rectificare a datelor inexacte şi de ştergere a datelor stocate în mod ilegal, răspunsurile autorităţilor competente trebuie transmise într-un termen limită. Astfel, persoana 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 legislaţia naţională.
De asemenea, persoana interesată va fi informată cu privire la rezultatul exercitării drepturilor acesteia de rectificare şi de ştergere 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 ştergere sau mai devreme, în cazul în care acest lucru este prevăzut de legislaţia naţională.

II.1. Dreptul de acces

Dreptul de acces reprezintă posibilitatea oricărei persoane care solicită acest lucru să aibă cunoştinţe despre informaţiile ce o privesc stocate într-un fişier de date prevăzut de legislaţia naţională. Acesta reprezintă un principiu fundamental de protecţie a datelor care permite persoanelor interesate să-şi exercite controlul asupra datelor cu caracter personal păstrate de terţi. Acest drept este prevăzut în mod expres în art. 41 din Regulamentul SIS II şi în art. 58 din Decizia SIS II .

Dreptul de acces este exercitat în conformitate cu legislaţia Statului Membru pe teritoriul căruia este înaintată cererea. Procedura şi regulile de comunicare a datelor către solicitant diferă de la un stat la altul. Când în Stat Membru primeşte o cerere de acces la o alertă emisă de alt stat, primul stat trebuie să ofere statului emitent ocazia de a-şi face cunoscută poziţia cu privire la posibilitatea dezvăluirii datelor către solicitant.

Informaţiile nu sunt comunicate către persoana vizată dacă acestea sunt indispensabile pentru efectuarea unei operaţiunii în legătură cu alerta sau pentru apărarea drepturilor şi libertăţilor unor terţi.

De asemenea, în prezent există două modalităţi de exercitare a dreptului de acces la datele prelucrate de autorităţile de aplicare a legii şi, prin urmare, aplicabile datelor SIS. În anumite State Membre dreptul de acces este direct, în alte este indirect.

II.1.1. Acces direct

În această situaţie persoana vizat se adresează direct autorităţilor ce prelucrează datele (poliţie, jandarmerie, vămi etc.). Daca legea naţională permite, solicitantul poate primi direct informaţiile referitoare la el.

II.1.2. Acces indirect

În această situaţie persoană se adresează autorităţii naţionale pentru protecţia datelor din statul unde se depune cererea. Autoritatea pentru protecţia datelor efectuează verificările necesare pentru a gestiona cererea şi oferă un răspuns solicitantului.

II.2. Dreptul de rectificare şi de ştergere a datelor

Pe lângă dreptul de acces, există, de asemenea, dreptul de rectificare a datelor personale inexacte sau incomplete sau dreptul de a solicita ştergerea datelor personale stocate în mod ilegal (art. 41(5) din Regulamentul SIS II) şi art. 58(5) din Decizia SIS II).

Potrivit cadrului legal Schengen numai Statul Membru responsabil pentru introducerea unei alerte în SIS o poate modifica sau şterge (vezi art. 34(2) din Regulamentul SIS II şi art. 49(2) din Decizia SIS II).

În situaţia în care solicitarea este transmisă altui Stat Membru decât cel care a emis alerta, autorităţile competente implicate vor coopera, prin schimbul de informaţii şi prin efectuarea de verificări necesare, în vederea soluţionării cazului.

Solicitantul va motiva cererea de rectificare sau ştergere a datelor şi va transmite orice informaţii relevante în susţinerea acesteia.

II.3. Căi de atac: dreptul de a înainta o plângere autorităţii pentru protecţia datelor sau de a se adresa justiţiei

Art. 43 din Regulamentul SIS II şi art. 59 din Decizia SIS II prezintă căile de atac accesibile persoanelor atunci când nu sunt mulţumite de răspuns. Orice persoană poate introduce o acţiune la instanţele judecătoreşti sau la autoritatea competentă potrivit legislaţiei naţionale pentru accesarea, rectificarea, ştergerea datelor sau pentru obţinerea de compensaţii în legătură cu o alertă care o priveşte.
În situaţia în care este vorba de o plângere cu un element transnaţional, autorităţile pentru protecţia datelor trebuie să coopereze pentru a garanta drepturile persoanelor vizate.

În ROMANIA

Potrivit art. 62 din Legea nr. 141/2010 *privind înfiinţarea, organizarea şi funcţionarea Sistemului Informatic Naţional de Semnalări şi participarea României la Sistemul de Informaţii Schengen*:

(1) Drepturile persoanei vizate în contextul prelucrării datelor cu caracter personal în SINS sau în SIS se exercită potrivit prevederilor Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, cu modificările şi completările ulterioare, cu derogările prevăzute de prezenta lege.

(2) **Cererile persoanelor vizate în contextul prelucrării datelor cu caracter personal în SINS sau în SIS se adresează numai Biroului SIRENE naţional**, care răspunde solicitantului cât mai curând posibil, dar nu mai târziu de 60 de zile de la data primirii cererii, în cazul exercitării dreptului de acces la datele personale, şi cât mai curând posibil, dar nu mai târziu de 90 de zile de la data primirii cererii, în cazul exercitării dreptului de rectificare şi ştergere a datelor personale, prin derogare de la prevederile Legii nr. 677/2001, cu modificările şi completările ulterioare.

(3) Cererile se pot depune la Biroul SIRENE naţional sau la orice operator din cadrul Ministerului Afacerilor Interne ori al unei structuri teritoriale a acestuia, care transmite cererea Biroului SIRENE naţional, în termen de 5 zile de la data primirii acesteia.

(4) Pentru a comunica solicitantului informaţii cu privire la datele cu caracter personal prelucrate în SINS sau în SIS, Biroul SIRENE naţional solicită acordul autorităţilor naţionale competente care au introdus semnalările în cauză. Acordul se comunică în termen de 20 de zile de la data primirii solicitării din partea Biroului SIRENE naţional.

(5) În cazul semnalărilor introduse în SIS de alt stat membru, cererile persoanelor vizate se soluţionează de către Biroul SIRENE naţional numai după solicitarea poziţiei statului membru care a introdus semnalarea. Biroul SIRENE naţional solicită poziţia prin schimbul de informaţii suplimentare.

(6) Biroul SIRENE naţional comunică, în termen de 40 de zile de la primirea solicitării, acordul cu privire la transmiterea de către un alt stat membru a datelor cu caracter personal cuprinse sau în legătură cu semnalările transmise de autorităţile naţionale competente în SIS, numai cu acordul acestora. Acordul se comunică în termen de 20 de zile de la data primirii solicitării din partea Biroului SIRENE naţional.

Adresa de corespondenţă:

Centrul de Cooperare Poliţienească Internaţională
Biroul SIRENE
1-5 Calea 13 Septembrie, Bucureşti, sectorul 5
România
Tel.: +40 21 315 96 26
Tel.: +40 21 314 05 40
Fax: +40 21 314 12 66
Fax: +40 21 312 36 00
E-mail: ccpi@mai.gov.ro

Legalitatea prelucrării datelor cu caracter personal în N.SIS pe teritoriul României şi transmiterea acestor date în străinătate, precum şi schimbul şi procesarea ulterioară a informaţiilor suplimentare sunt monitorizate şi se supun controlului A.N.S.P.D.C.P.
Auditarea operaţiunilor de prelucrare a datelor cu caracter personal în N.SIS se efectuează de către A.N.S.P.D.C.P., în conformitate cu standardele internaţionale de audit, cel puţin o dată la 4 ani.

Adresa de corespondenţă:
Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal
Bd. G-ral Gheorghe Magheru nr. 28-30
Sector 1, Bucureşti
România
Tel.: +40 31 805 92 11
Fax: +40 31 805 96 02
E-mail: anspdcp@dataprotection.ro

Regimul limbajului

Persoana vizată, cetăţean român, poate transmite solicitarea în limba română, iar cetăţenii străini pot transmite solicitarea în engleză.