Sistemul de informații Schengen II – Ghid privind exercitarea dreptului de acces
Rezumat

Persoanele ale căror date cu caracter personal sunt culese, păstrate sau prelucrate în orice alt mod în Sistemul de informații Schengen de a doua generație (denumit în continuare „SIS II") beneficiază de drepturi de acces, de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal[1]. Ghidul de față descrie modalitățile în care pot fi exercitate aceste drepturi.

I. Prezentarea sistemului de informații Schengen de a doua generație (SIS II)

SIS II este un sistem informatic la scară largă, înființat ca măsură compensatorie pentru eliminarea controalelor la frontierele interne, și are scopul de a asigura un nivel ridicat de securitate în cadrul spațiului de libertate, securitate și justiție al Uniunii Europene, inclusiv prin menținerea siguranței și ordinii publice și garantarea securității pe teritoriul statelor membre. SIS II este implementat în toate statele membre ale UE cu excepția Ciprului, a Croației și a Irlandei[2], precum și în patru state asociate: Islanda, Norvegia, Elveția și Liechtenstein.

SIS II este un sistem informatic care permite autorităților naționale de aplicare a legii, judiciare și administrative să efectueze sarcini specifice prin schimbul de date relevante. Agențiile europene EUROPOL și EUROJUST au, de asemenea, drepturi de acces limitat la sistem.

Categorii de informații prelucrate

SIS II centralizează două mari categorii de informații, care se prezintă sub forma unor alerte, în primul rând cu privire la *persoane* – fie persoane căutate în vederea arestării, dispărute, căutate în vederea participării la o procedură judiciară sau pentru efectuarea de controale discrete sau specifice, fie resortisanți ai unor țări terțe vizați de interdicții de intrare sau de ședere în spațiul Schengen, și în al doilea rând cu privire la *obiecte* – cum ar fi vehicule, documente de călătorie sau carduri de credit, căutate pentru a fi confiscate sau folosite ca probe în cursul procedurilor penale sau în vederea unor controale discrete sau specifice.

Temei juridic

În funcție de tipul alertei, SIS II este reglementat fie prin Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen din a doua generație (denumit în continuare „Regulamentul SIS II"), în ceea ce privește procedurile de emitere a alertelor care intră sub incidența titlului IV din Tratatul de instituire a Comunității Europene – fostul pilon I, fie prin Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (denumită în continuare „Decizia SIS II"), în ceea ce privește procedurile care intră sub incidența titlului VI din Tratatul privind Uniunea Europeană – fostul pilon III.

[1] Aceste drepturi sunt acordate în temeiul articolului 41 din Regulamentul (CE) nr. 1987/2006 din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen din a doua generație (SIS II) și al articolului 58 din Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II).

[2] Informații din iulie 2015. Deși folosesc sistemul SIS, Bulgaria și România au în continuare frontiere interne. Regatul Unit are acces la SIS, cu excepția alertelor emise în scopul neadmiterii pe teritoriul Schengen.

Categorii de date cu caracter personal prelucrate

Atunci când alerta se referă la o persoană, informațiile trebuie să cuprindă întotdeauna numele, prenumele și eventualele pseudonime, sexul, o trimitere la decizia care a dus la emiterea alertei și măsurile care trebuie luate. Dacă sunt disponibile, alerta poate conține și informații precum: orice caracteristici fizice specifice, obiective, care nu se pot modifica; locul și data nașterii; fotografii; amprente digitale; cetățenia (cetățeniile); dacă persoana în cauză este înarmată, violentă sau a evadat; motivul alertei; autoritatea care a emis alerta; legătura cu alte alerte emise în SIS II în conformitate cu articolul 37 din Regulamentul SIS II sau cu articolul 52 din Decizia SIS II.

Arhitectura sistemului

SIS II este format din: (1) un sistem central („SIS II central"); (2) un sistem național („N.SIS II") în fiecare stat membru, care comunică cu SIS II central; și (3) o infrastructură de comunicații între sistemul central și sistemele naționale care furnizează o rețea virtuală criptată dedicată datelor din SIS II și schimbului de date între autoritățile însărcinate cu schimbul tuturor informațiilor suplimentare (birourile SIRENE)[3].

II. Drepturi acordate persoanelor fizice ale căror date sunt prelucrate în SIS II

În conformitate cu principiile privind protecția datelor, toate persoanele fizice ale căror date sunt prelucrate în SIS II beneficiază de drepturi specifice, acordate prin Regulamentul SIS II și Decizia SIS II[4], care vor fi analizate mai jos. Orice persoană care își exercită unul dintre aceste drepturi poate să apeleze la autoritățile competente ale unuia dintre statele care utilizează SIS II, la alegerea sa. Această opțiune este posibilă deoarece toate bazele de date naționale (N.SIS II) sunt identice cu baza de date a sistemului central[5]. Prin urmare, aceste drepturi pot fi exercitate în orice țară în care se utilizează SIS II, indiferent de statul membru care a emis alerta.

Atunci când o persoană își exercită dreptul de acces, de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal, autoritățile competente au obligația să răspundă într-un anumit termen strict. Astfel, persoana interesată este informată cât mai curând posibil și, în orice caz, în termen de cel mult 60 de zile de la data cererii de acces la date, sau mai devreme în cazul în care legislația națională prevede un termen mai scurt[6]. Astfel, persoana interesată este informată cât mai curând posibil și, în orice caz, în termen de cel mult 60 de zile de la data cererii de acces la date, sau mai devreme în cazul în care legislația națională prevede un termen mai scurt[7].

[3] Datele sunt introduse, actualizate, șterse și căutate în SIS II prin intermediul diferitelor sisteme naționale. Sistemul central, care asigură controlul tehnic și îndeplinește funcții administrative, se află la Strasbourg (Franța). Acesta oferă serviciile necesare pentru introducerea și prelucrarea datelor din SIS II. Există și un sistem central de rezervă, capabil să asigure toate funcționalitățile sistemului central principal în cazul defectării acestuia și amplasat în apropiere de Salzburg (Austria). Fiecare stat membru răspunde de înființarea, funcționarea și întreținerea propriului sistem național și de conectarea lui la sistemul central. Fiecare stat desemnează o autoritate, oficiul național SIS II (oficiul N.SIS II), care își asumă responsabilitatea principală pentru proiectul SIS II național. Această autoritate răspunde de buna funcționare și de securitatea propriului sistem național.

[4] A se vedea, în special, articolul 41 din Regulamentul SIS II și articolul 58 din Decizia SIS II.

[5] A se vedea articolul 4 alineatul (1) litera (b) din Regulamentul și Decizia SIS II.

[6] A se vedea articolul 41 alineatul (6) din Regulamentul SIS II și articolul 58 alineatul (6) din Decizia SIS II.

[7] A se vedea articolul 41 alineatul (7) din Regulamentul SIS II și articolul 58 alineatul (7) din Decizia SIS II.

Dreptul de acces

Dreptul de acces se referă la posibilitatea oricărei persoane care solicită acest lucru de a avea acces la informațiile care o privesc stocate într-un fișier de date, în conformitate cu legislația națională. Acesta este un principiu fundamental de protecție a datelor, care permite persoanelor vizate să își exercite controlul asupra datelor cu caracter personal deținute de terți. Acest drept este prevăzut în mod expres la articolul 41 din Regulamentul SIS II și la articolul 58 din Decizia SIS II.

Dreptul de acces se exercită în conformitate cu legislația statului membru în care se depune cererea. Procedurile, ca și normele de comunicare a datelor către solicitant, diferă de la o țară la alta. În cazul în care un stat membru primește o cerere de acces la o alertă emisă de alt stat, el trebuie să permită țării emitente să își exprime poziția cu privire la posibilitatea de a comunica datele solicitantului[8]. Informațiile nu se comunică persoanei vizate în cazul în care sunt indispensabile pentru îndeplinirea sarcinii juridice asociate alertei sau pentru protejarea drepturilor și libertăților altor persoane.

În prezent, există două tipuri de sisteme care reglementează dreptul de acces la datele prelucrate de autoritățile de aplicare a legii și care, prin urmare, sunt aplicabile și datelor SIS. În unele state membre dreptul de acces este direct, iar în altele – indirect.

În cazul **accesului direct**, persoana interesată transmite solicitarea direct autorităților care gestionează datele (poliție, jandarmerie, autorități vamale etc.). Dacă legislația națională o permite, solicitantului îi pot fi transmise informațiile care îl privesc.

În cazul **accesului indirect**, persoana în cauză transmite solicitarea de acces către autoritatea națională pentru protecția datelor din statul căruia îi este adresată solicitarea. Autoritatea pentru protecția datelor efectuează verificările necesare pentru a da curs cererii și transmite răspunsul solicitantului.

Dreptul de rectificare și de ștergere a datelor

Pe lângă dreptul de acces, persoanele beneficiază de dreptul de a obține rectificarea datelor cu caracter personal care conțin erori de fapt sau sunt incomplete, precum și de dreptul de a solicita ștergerea datelor care le privesc dacă acestea sunt stocate în mod ilegal [articolul 41 alineatul (5) din Regulamentul SIS II și articolul 58 alineatul (5) din Decizia SIS II].

În conformitate cu cadrul juridic Schengen, numai statul care emite o alertă în SIS II poate modifica sau șterge această alertă [a se vedea articolul 34 alineatul (2) din Regulamentul SIS II și articolul 49 alineatul (2) din Decizia SIS II]. În cazul în care cererea este depusă într-un alt stat membru, autoritățile competente ale statelor membre în cauză cooperează în vederea soluționării cazului, făcând schimb de informații și efectuând verificările necesare. Solicitantul trebuie să precizeze motivele care stau la baza cererii sale de rectificare sau ștergere a datelor și să obțină toate informațiile relevante în sprijinul acesteia.

Căi de atac: dreptul de a înainta o plângere autorității pentru protecția datelor sau de a iniția proceduri judiciare

Articolul 43 din Regulamentul SIS II și articolul 59 din Decizia SIS II prevăd căile de atac de care dispun persoanele fizice în cazul în care nu se dă curs solicitărilor acestora. Orice persoană poate să introducă o acțiune în fața instanțelor judecătorești sau a autorității

[8] A se vedea articolul 41 alineatul (3) din Regulamentul SIS II și articolul 58 alineatul (3) din Decizia SIS II.

competente în temeiul legislației naționale a oricărui stat membru pentru a avea acces, a rectifica, a șterge date sau a obține informații sau compensații în legătură cu o alertă care o privește.

În cazul plângerilor care conțin elemente transfrontaliere, autoritățile naționale pentru protecția datelor ar trebui să coopereze pentru a garanta respectarea drepturilor persoanelor vizate.