

Ministerul Administrației și Internelor

Protecția datelor cu caracter personal în SIS

Cuprins

Acquis relevant.....	4
Cadrul legislativ intern actual.....	5
Transpunerea acquis-ului comunitar la nivel national	5
Ce reprezintă Sistemul Informatic Schengen ?.....	6
Reguli generale privind datele introduse în SIS	7
Categoriile de date personale introduse în SINS	8
Elemente cuprinse în datele cu caracter personal introduse în SIS	9
Consimțământul persoanei ale cărei date personale sunt prelucrate	10
Autorități naționale competente în gestionarea și exploatarea SINS	11
Măsuri tehnice pentru asigurarea protecției datelor personale	12
Drepturile persoanei în contextul prelucrării datelor personale	13
Excepție.....	14
Introducerea cererii/formularului de către solicitant cu privire la drepturile sale	15
Soluționarea cererii introduse de solicitant cu privire la drepturile sale	15
Informarea solicitantului cu privire la alte drepturi.....	16
Plângeri adresate autorității naționale de supraveghere	17
Informații utile despre spațiul Schengen.....	18
Definiții	19

Conceptul de **protecție a datelor cu caracter personal** reprezintă dreptul persoanei fizice de a-i fi apărate acele caracteristici care conduc la identificarea sa și obligația corelativă a statului de a adopta măsuri adecvate pentru a asigura o protecție eficientă.

Prin date cu caracter personal se înțeleg acele informații care pot fi puse direct sau indirect în legătură cu o persoană fizică identificată sau identificabilă, cum ar fi cu titlu de exemplu, **numele, prenumele, cod numeric personal, adresa, telefon, imaginea, etc.**

Având în vedere necesitatea de a apăra și respecta dreptul fundamental la viață intimă și privată, **protecția datelor cu caracter personal** constituie un domeniu deosebit de important fapt confirmat prin tratarea acestei tematici în capitole distincte prevăzute în Convenția de Aplicare a Acordului Schengen.

ACQUIS RELEVANT

Obiectivul prevederilor acquis-ului comunitar privind prelucrarea datelor cu caracter personal, avut în vedere cu ocazia transpunerii acestora în legislația națională, este reprezentat de **garantarea și protejarea drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viață intimă, familială și privată.**

Dreptul fundamental la viață intimă și privată este garantat de

- ☞ Tratatul privind instituirea Uniunii Europene (TUE), articolul 6
- ☞ Carta UE a Drepturilor Fundamentale, 7 decembrie 2000
- ☞ Convenția Europeană pentru protecția Drepturilor și Libertăților Fundamentale ale Omului (ECHR), articolul 8

A. Pilonul I

- Convenția de Aplicare a Acordului Schengen – **art. 126 – 130**- protecția datelor cu caracter personal;
- Convenția Consiliului European 108/1981 privind protecția persoanelor cu privire la procesarea automată a datelor personale (Strasbourg, 28 ianuarie 1981);
- Protocolul adițional al Convenției privind autoritățile de supraveghere și fluxurile de date trans-frontaliere (4 octombrie 2001);
- Directiva Consiliului 1995/46/EC a Parlamentului European și a Consiliului European din 24 octombrie 1995 cu privire la protecția persoanelor referitoare la procesarea datelor personale și la libera circulație a acestor date;
- Regulamentul (EC) nr. 45/2001 al Parlamentului European și al Consiliului privind protecția persoanelor cu privire la procesarea datelor personale de către instituțiile și organismele comunitare și la libera circulație a acestor date;
- Directiva 2002/58/EC a Parlamentului European și a Consiliului din 12.07.2002 privind procesarea datelor personale și protecția intimității în sectorul comunicațiilor electronice.

B. Pilonul III

- Convenția de Implementare a Acordului Schengen – **art. 102-118¹**-protecția datelor personale în SIS ;
- Recomandarea 1987 (15) a Comitetului de Miniștri adresată statelor membre, pentru reglementarea utilizării datelor personale în activitatea poliției;

¹ amendată de: Regulamentul Consiliului 2004/871 și de Decizia Consiliului 2005/211

* art. 102a a fost introdus prin Regulamentul Parlamentului European și Consiliului 2005/1160 și înlocuit de Regulamentul Parlamentului European și Consiliului 2006/1986

* art. 102 - 118 au fost înlocuite de Regulamentul Parlamentului European și al Consiliului 2006/1987 și de Decizia Consiliului 2007/533 (pentru Statele Membre participante la SIS 1 +)

ATENȚIE! Acquis-ul Schengen în domeniu nu vizează datele/informațiile cu caracter secret sau documente clasificate.

CADRUL LEGISLATIV INTERN ACTUAL

Transpunerea acquis-ului comunitar la nivel national

Protecția datelor personale - Art. 126 – 130 CAAS

- Constituția României, art 26
- Legea nr. 682/2001 privind ratificarea de către România a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981(MOf);
- Legea nr 55/2001 pentru ratificarea Protocolului Aditional al Convenției privind autoritățile de supraveghere și fluxurile de date trans-frontaliere, adoptata la Strasbourg, 19 noiembrie 2001, CETS no 181 ;
- Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare;
- Legea nr. 102/2005 privind înființarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Protecția datelor personale în SIS- Art. 102-118 din CAAS

- O.U.G. nr. 128/2005 privind înființarea, organizarea și funcționarea Sistemului Informatic Național de Semnalări;
- Hotărârea nr 1411 din 11.10.2006 pentru aprobarea Normelor de aplicare a Ordonanței de urgență a Guvernului nr. 128/2005 privind înființarea, organizarea și funcționarea Sistemului Informatic National de Semnalări;
- Legea nr. 345 din 29 noiembrie 2005 pentru aprobarea Ordonanței de urgență a Guvernului nr. 128/2005 privind înființarea, organizarea și funcționarea Sistemului Informatic National de Semnalări

🔔 Aceste acte normative sunt în curs de modificare pentru a se asigura compatibilitatea cu legislația comunitară în domeniul SIS II, respectiv Decizia Consiliului 2007/533 privind înființarea, funcționarea și utilizarea Sistemului Informatic Schengen de a doua generație (SIS II).

🔔 De asemenea, Recomandarea nr.(87)15 a Comitetului de Miniștri al Consiliului Europei privind utilizarea datelor cu caracter personal în domeniul poliției este transpusă prin act normativ.

CE REPREZINTĂ SISTEMUL INFORMATIC SCHENGEN ?

Sistemul Informatic Schengen (SIS) reprezintă o bază de date electronică de interes polițienesc care permite autorităților competente din statele membre să coopereze în vederea menținerii ordinii publice și securității naționale pe teritoriile statelor membre, folosind informații comunicate prin intermediul acestui sistem.

În prezent, SIS reunește cca 15 milioane de semnalări introduse de statele membre. Toate statele membre introduc date în sistem direct de la bazele de date naționale.

Sistemul Informatic Schengen actual a fost construit pentru 18 state (15 state membre, Islanda, Norvegia și un loc de rezervă), arhitectură depășită de noua configurație a Uniunii Europene.

Noile descoperiri tehnice, noile nevoi apărute pe parcursul operării SIS, noul context legal apărut după Tratatul de la Amsterdam și lărgirea Uniunii Europene, au impus dezvoltarea celei de-a doua generații a SIS.

SIS II este compus dintr-un sistem central (numit C.SIS II), o secțiune națională (N.SIS) și o infrastructură de comunicații între C.SIS și N.SIS. Toate sistemele naționale sunt conectate online cu sistemul central, localizat la Strasbourg.

Ca etapa prealabilă în procesul de implementarea a SIS II, în România se va înființa Sistemul Informatic Național de Semnalări (SINS) care conține semnalările de interes național și de interes Schengen emise de către autoritățile naționale competente.

SINS permite autorităților naționale competente ca prin intermediul unei proceduri de căutare automată în sistem să aibă acces la semnalările cu privire la persoane și bunuri, în scopul îndeplinirii atribuțiilor specifice în domeniile controlului trecerii frontierei de stat, al respectării regimului vamal, al eliberării vizelor și permiselor de ședere, precum și al celorlalte controale și activități specifice efectuate de organele de poliție sau de către alte autorități în scopul asigurării ordinii și siguranței publice și a securității naționale.

REGULI GENERALE PRIVIND DATELE INTRODUSE ÎN SIS

Datele din SIS pot fi copiate numai în scopuri tehnice, cu condiția ca această copiere să fie necesară pentru ca autoritățile competente să poată efectua o căutare directă.

Datele nu pot fi utilizate în scopuri administrative.

Semnalarea introdusă în SIS nu poate fi suplimentată, corectată sau modificată decât de autoritatea care a introdus-o. Alertele din SIS pot fi însă accesate de către toate statele membre ale spațiului Schengen, respectiv de către autoritățile abilitate prin lege din respectivele state membre.

Fiecare stat membru se va asigura că fiecare transmitere a datelor cu caracter personal este înregistrată în secțiunea națională a SIS de autoritatea de management a fișierului de date în scopul verificării dacă acea căutare este admisibilă sau nu.

Datele cu caracter personal introduse în SIS sunt stocate numai pe perioada necesară atingerii scopului pentru care au fost introduse.

La nivel național, toate tranzacțiile efectuate asupra datelor din SINS sunt înregistrate în sistem în scopul verificării legalității căutării, monitorizării, legalității prelucrării datelor, asigurării funcționării corespunzătoare a SINS precum și a integrității și securității datelor.

Înregistrările privind tranzacțiile pot fi folosite numai în scopul susmenționat și sunt șterse după cel puțin un an și cel mult 3 ani de la creare. Înregistrările pot fi păstrate pentru o perioadă mai îndelungată, dacă sunt necesare pentru procedurile de monitorizare care se află deja în curs de desfășurare.

Toate stările prin care trec semnalările, de la momentul introducerii lor în SINS și până la momentul ștergerii lor din SINS, se înregistrează în istoricul semnalărilor în scopul monitorizării și al verificării legalității prelucrării datelor.

Înregistrările arată data și ora transmisiei de date, datele folosite pentru efectuarea unei căutări, o referință cu privire la datele transmise, numele autorității competente și al persoanei care a efectuat procesarea datelor.

CATEGORII DE DATE PERSONALE INTRODUSE ÎN SINS

☞ date 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;

☞ date cu privire la cetățenii statelor terțe împotriva cărora s-a dispus măsura nepermitterii intrării sau șederii, în conformitate cu art. 24, 25 și 26 din Regulamentul Parlamentului European și al Consiliului privind instituirea, operaționalizarea și utilizarea SIS de a doua generație (SIS II);

☞ date privind persoanele dispărute:

a) care trebuie plasate sub protecție, în baza unei hotărâri emise de o autoritate competentă, pentru propria lor protecție sau pentru a preîntâmpina amenințările;

b) care nu trebuie plasate sub protecție dar a căror locație trebuie stabilită

☞ date privind persoanele căutate în vederea participării la o procedură judiciară, al căror domiciliu sau reședință trebuie stabilite, în următoarele cazuri:

- persoanele citate ca martori de către autoritățile judiciare;
- persoanele citate sau căutate pentru a fi citate în vederea prezentării în fața autorităților judiciare în legătură cu o procedură penală pentru a răspunde cu privire la fapte pentru care s-a dispus începerea urmăririi penale;
- persoane cărora trebuie să li se înmâneze o sentință penală sau alte documente privind o procedură judiciară pentru a răspunde în legătură cu fapte pentru care s-a dispus începerea urmăririi penale;
- persoane cărora li se va înmâna o citație pentru a se prezenta în scopul executării unei pedepse privative de libertate;

☞ date privind persoanele care fac obiectul unor controale discrete, în scopul urmăririi penale sau al executării pedepsei penale și pentru prevenirea amenințărilor la adresa securității publice și siguranței naționale.

ELEMENTE CUPRINSE ÎN DATELE CU CARACTER PERSONAL INTRODUSE ÎN SIS

- ☞ numele și prenumele, numele la naștere și numele anterior, orice pseudonime care pot fi introduse separat
- ☞ semnele fizice particulare, obiective și inalterabile
- ☞ data și locul nașterii
- ☞ sexul
- ☞ fotografiile²
- ☞ amprentele digitale³
- ☞ cetățenia
- ☞ mențiunea că persoana vizată este înarmată, violentă sau evadată
- ☞ motivul semnalării
- ☞ autoritatea care emite semnalarea
- ☞ decizia sau hotărârea care a stat la baza semnalării
- ☞ măsurile care trebuie luate
- ☞ legătura cu alte semnalări emise
- ☞ tipul infracțiunii

☞ Utilizatorii datelor personale trebuie să acceseze numai datele personale necesare pentru îndeplinirea atribuțiilor de serviciu

^{2 3} Fotografiile și amprentele digitale, ca date adiționale ale semnalării, se introduc în măsura în care sunt disponibile și sunt folosite doar pentru confirmarea identității unei persoane care a fost localizată, ca urmare a realizării unui rezultat pozitiv.

CONSIMȚĂMÂNTUL PERSOANEI ALE CĂREI DATE PERSONALE SUNT PRELUCRATE

Orice prelucrare de date cu caracter personal, cu excepția prelucrărilor care vizează date din categoriile menționate de lege, poate fi efectuată numai dacă persoana vizată și-a dat consimțământul în mod expres și neechivoc pentru acea prelucrare.

Dintre excepțiile stipulate de lege, menționăm situațiile în care consimțământul persoanei vizate nu este necesar atunci când prelucrarea se efectuează:

- *în vederea protejării vieții, integrității fizice sau sănătății persoanei vizate ori a unei alte persoane amenințate*
- *în vederea îndeplinirii unei obligații legale a operatorului*
- *în vederea aducerii la îndeplinire a unor măsuri de interes public sau care vizează exercitarea prerogativelor de autoritate publică cu care este investit operatorul sau terțul căruia îi sunt dezvăluite datele.*

AUTORITĂȚI NAȚIONALE COMPETENTE ÎN GESTIONAREA ȘI EXPLOATAREA SINS

Ministerul Administrației și Internelor, prin structura sa de specialitate, este autoritatea publică centrală care **gestionează și răspunde de buna funcționare a SINS**, de integritatea semnalărilor conținute în acesta, conform exigențelor acquis-ului Schengen, asigurând accesul autorităților naționale competente din România la SINS.

Gestiunea și utilizarea datelor conținute în SINS, cu privire la prelucrarea datelor cu caracter personal, **sunt supuse controlului de către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)**. La nivel național, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal este autoritatea publică cu personalitate juridică, autonomă și independentă față de orice altă autoritate a administrației publice, ca și față de orice persoana fizică sau juridică din domeniul privat. În același timp, este singura autoritate care are atribuții de control, investigații și supraveghere în domeniu. Președintele Autorității naționale de supraveghere, în exercitarea atribuțiilor sale, emite decizii și instrucțiuni obligatorii pentru toate instituțiile și unitățile la a căror activitate se referă.

Autoritățile naționale competente să introducă date în SINS sunt acele autorități care au atribuții în furnizarea și/sau consultarea semnalărilor conținute în SINS. În prezent, acestea sunt prevăzute de Ordonanța de Urgență nr. 128 din 15 septembrie 2005 privind înființarea, organizarea și funcționarea Sistemului Informatic Național de Semnalări, după cum urmează:

- ☞ Poliția Română;
- ☞ Poliția de Frontieră Română;
- ☞ Jandarmeria Română;
- ☞ Oficiul Român pentru Imigrări;
- ☞ Biroul SIRENE, de la data operaționalizării acestuia;
- ☞ Inspectoratul Național pentru Evidența Persoanelor;
- ☞ Direcția Generală de Pașapoarte;
- ☞ Direcția Regim Permise de Conducere și Înmatriculare a Vehiculelor;
- ☞ Autoritatea Națională a Vămilelor;
- ☞ Ministerul Afacerilor Externe;
- ☞ Ministerul Justiției.

<p>Autoritățile naționale competente consultă numai semnalările conținute în SINS necesare în vederea îndeplinirii propriilor atribuții și asigură accesul la acestea numai personalului autorizat în acest sens, în limitele competențelor profesionale.</p>
--

MĂSURI TEHNICE PENTRU ASIGURAREA PROTECȚIEI DATELOR PERSONALE

Fiecare autoritate națională competentă este obligată să adopte măsuri necesare pentru a asigura un nivel de protecție adecvat a datelor cu caracter personal.

- a) a împiedica accesul persoanelor neautorizate la echipamentele de prelucrare a datelor folosite pentru prelucrarea datelor cu caracter personal (controlul accesului la echipamente);
- b) a împiedica citirea, copierea, modificarea sau eliminarea neautorizată a suportului de date (controlul suportului de date);
- c) a împiedica introducerea neautorizată de date și inspectarea, modificarea sau ștergerea neautorizată a datelor cu caracter personal (controlul stocării);
- d) a împiedica utilizarea sistemelor de prelucrare automată a datelor de către persoane neautorizate cu ajutorul echipamentelor de comunicare a datelor (controlul utilizatorului);
- e) a asigura că persoanele autorizate să utilizeze un sistem de prelucrare automată a datelor au acces numai la datele pentru care au autorizare (controlul accesului la date);
- f) a se asigura că este posibil să verifice și să stabilească organismele cărora le pot fi transmise datele cu caracter personal folosind echipamentele de comunicare a datelor (controlul comunicării);
- g) 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);
- h) a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transmiterii de date cu caracter personal sau în timpul transportului de suporturi de date (controlul transportului).

DREPTURILE PERSOANEI ÎN CONTEXTUL PRELUCRĂRII DATELOR PERSONALE

În conformitate cu principiile protecției datelor, drepturile specifice persoanelor sunt recunoscute de Convenția de Aplicare a Acordului Schengen.

Orice persoană are dreptul de a avea acces la datele personale introduse în SIS, potrivit legislației naționale, dacă ele solicită acest lucru.

Orice persoană are dreptul să solicite autorităților de control verificarea datelor introduse în Sistemul de Informații Schengen cu privire la ea însăși și modul în care au fost folosite aceste date.

Acest drept este reglementat de legislația națională a părții contractante căreia i se adresează solicitarea. Dacă datele au fost introduse de o altă parte contractantă, verificarea se efectuează în strânsă coordonare cu autoritatea de control a acelei părți contractante.

Constituția României recunoaște drepturile cetățenilor la viață intimă, familială și privată, indiferent de naționalitatea acestora, fără a face distincție între cetățenii români, cetățenii străini și apatrizii care locuiesc în România.

Legea nr. 677/2001 cu completările și modificările ulterioare prevede drepturile specifice ale persoanei în contextul prelucrării datelor cu caracter personal

↳ **Dreptul la informare** – operatorul este obligat să încunoștințeze persoana vizată cu privire la prelucrarea datelor sale cu caracter personal.

↳ **Dreptul de acces la date** – orice persoană vizată are dreptul de a obține de la operator, la cerere (în mod gratuit, pentru o solicitare pe an), confirmarea faptului că datele sale personale sunt sau nu sunt prelucrate de către acesta.

↳ **Dreptul de intervenție asupra datelor** – orice persoană vizată are dreptul de a obține de la operator, în mod gratuit, rectificarea, actualizarea, blocarea sau ștergerea datelor a căror prelucrare nu este conformă legii, în special a datelor incomplete sau inexacte.

↳ **Dreptul de opoziție** - persoana vizată are dreptul de a se opune în orice moment, printr-o cerere întocmită în formă scrisă, datată și semnată, din motive întemeiate și legitime legate de situația sa particulară, ca datele care o vizează să facă obiectul unei prelucrări.

↳ **Dreptul de a nu fi supus unei decizii individuale luate în baza unei prelucrări automate** - retragerea sau anularea oricărei decizii care produce efecte juridice în privința sa, adoptată exclusiv pe baza unei prelucrări de date cu caracter personal, efectuată prin mijloace automate.

↳ **Dreptul de a se adresa justiției** - orice persoană care a suferit un prejudiciu în urma unei prelucrări de date cu caracter personal, efectuate ilegal, se poate adresa instanței competente pentru repararea acestuia.

EXCEPȚIE

Prevederile referitoare la dreptul la informare, dreptul de acces la date, dreptul la opoziție precum și obligația operatorului de a comunica numele terțului căruia i-au fost dezvăluite datele cu caracter personal *nu se aplică prelucrărilor și transferului de date cu caracter personal, efectuate în cadrul activităților de prevenire, cercetare și reprimare a infracțiunilor și de menținere a ordinii publice, precum și a altor activități desfășurate în domeniul dreptului penal, în limitele și cu restricțiile stabilite de lege.*

Astfel, în situația prezentată mai sus, autoritățile de aplicare a legii nu sunt obligate să informeze persoana vizată despre prelucrarea datelor sale cu caracter personal.

Această excepție de la obligațiile operatorului nu are însă caracter permanent având în vedere faptul că prevederile legislative sunt aplicabile strict pentru perioada necesară atingerii obiectivului urmărit prin desfășurarea activităților susmenționate.

După încetarea situației, operatorul trebuie să ia măsurile necesare pentru asigurarea drepturilor persoanei vizate.

INTRODUCEREA CERERII/FOMULARULUI DE CĂTRE SOLICITANT CU PRIVIRE LA DREPTURILE SALE

Cu privire la drepturile sale, orice persoană (solicitant) se poate adresa direct operatorului printr-o cerere/formular întocmit(ă) în formă scrisă, datat(ă) și semnat(ă).

Solicitantul poate preciza în cerere dacă dorește ca informațiile să îi fie comunicate la o anumită adresă, care poate fi și de poștă electronică, sau printr-un serviciu de corespondență care să asigure că predarea i se va face numai personal.

În cazul în care cererea se depune prin reprezentant, se solicită datele de identificare ale reprezentantului precum și împuternicirea.

Cererea se depune la registratura fiecărui operator de date cu caracter personal, unde, în aceeași zi, sunt trecute în registrul general de intrare-ieșire a corespondentei și primesc număr și data de înregistrare. Numărul și data de înregistrare a cererii pe care solicitantul a completat-o conform celor prevăzute mai sus pot fi comunicate de operator numai la solicitarea expresă a acestuia.

SOLUȚIONAREA CERERII INTRODUSE DE SOLICITANT CU PRIVIRE LA DREPTURILE SALE

Operatorul este obligat să comunice informațiile solicitate, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opțiuni a solicitantului exprimate în cerere.

În ceea ce privește drepturile specifice ale persoanei în contextul prelucrării datelor cu caracter personal din SIS, 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) precizează că persoana interesată este informată cât mai curând posibil și, în orice caz, într-un termen care nu depășește 60 de zile de la data la care depune cererea de acces și 90 zile pentru dreptul de intervenție asupra datelor.

De exemplu, în cazul solicitării dreptului de acces, operatorul este obligat, în situația în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia, împreună cu confirmarea, în termenul legal, cel puțin următoarele:

a) informații referitoare la scopurile prelucrării, categoriile de date avute în vedere și destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele;

b) comunicarea într-o formă inteligibilă a datelor care fac obiectul prelucrării, precum și a oricărei informații disponibile cu privire la originea datelor;

c) informații asupra principiilor de funcționare a mecanismului prin care se efectuează orice prelucrare automată a datelor care vizează persoana respectivă;

d) informații privind existența dreptului de intervenție asupra datelor și a dreptului de opoziție, precum și condițiile în care pot fi exercitate;

e) informații asupra posibilității de a consulta registrul de evidență a prelucrărilor de date cu caracter personal, de a înainta plângere către autoritatea de supraveghere, precum și de a se adresa instanței pentru atacarea deciziilor operatorului.

INFORMAREA SOLICITANTULUI CU PRIVIRE LA ALTE DREPTURI

Operatorul de date cu caracter personal informează solicitantul asupra dreptului de a se adresa justiției, în situația în care acesta a suferit un prejudiciu în urma unei prelucrări de date cu caracter personal, efectuată ilegal, fără ca prin aceasta să se aducă atingere posibilității solicitantului de a se adresa cu plângere Autorității Naționale de Supraveghere.

Instanța competentă este cea în a cărei rază teritorială domiciliază reclamantul. Cererea de chemare în judecată este scutită de taxă de timbru.

Operatorul de date cu caracter personal informează solicitantul asupra dreptului de a se adresa direct ANSPDCP cu privire la introducerea plângerilor legate de datele personale, sens în care operatorul de date cu caracter personal furnizează persoanei vizate datele de contact ale ANSPDCP (adresa, telefon, fax, adresa de email).

În ceea ce privește datele personale conținute în Sistemul Informatic Național de Semnalări, orice persoană interesată poate solicita Ministerului Administrației și Internelor, în condițiile legii, informații cu privire la datele cu caracter personal existente în SINS, care o vizează. Orice persoană prejudiciată prin introducerea sau exploatarea datelor cu caracter personal în SINS poate solicita, potrivit legii, repararea prejudiciului astfel cauzat.

PLÂNGERI ADRESATE AUTORITĂȚII NAȚIONALE DE SUPRAVEGHERE

În cazul în care persoanele ale căror date cu caracter personal sunt prelucrate consideră că drepturile prevăzute de Legea nr. 677/2001 le-au fost încălcate, acestea se pot adresa în scris autorității naționale de supraveghere cu condiția de a nu fi introdus anterior o acțiune în justiție, cu același obiect, însă numai după ce s-au adresat în prealabil operatorului reclamat.

Plângerea poate fi adresată direct sau prin reprezentant la ANSPDCP. Persoana vizată poate împuternici o asociație sau fundație să îi reprezinte interesele.

În afara cazurilor în care o întârziere ar cauza un prejudiciu iminent și ireparabil, plângerea către autoritatea de supraveghere nu poate fi înaintată mai devreme de 15 zile de la înaintarea unei plângeri cu același conținut către operator.

În cazul în care plângerea este găsită întemeiată, autoritatea națională de supraveghere poate dispune, în cazul în care constată încălcarea dispozițiilor prezentei legi, suspendarea provizorie sau încetarea prelucrării datelor, ștergerea parțială ori integrală a datelor prelucrate .
Decizia trebuie motivată și se comunică părților interesate în termen de 30 de zile de la data primirii plângerii.

Autoritatea de supraveghere se poate adresa justiției pentru apărarea oricăror drepturi ale persoanelor vizate, garantate de Legea 677/2001, completată și modificată.

Pentru mai multe detalii legate de protecția datelor, vă rugăm vizitați site-ul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal - www.dataprotection.ro.

INFORMAȚII UTILE DESPRE SPAȚIUL SCHENGEN



I. Ce este Schengen?

Mică localitate de frontieră din Luxemburg.

În anul 1985 a fost încheiat un **acord** privind eliminarea treptată a controalelor la frontiera comună **între Germania, Franța, Țările de Jos, Belgia și Luxemburg**, pe nava "Astrid" pe râul Mosel, în dreptul localității Schengen.

II. Ce reprezintă spațiul Schengen?

Zonă de libertate de mișcare unde controalele la frontierele interne ale statelor semnatare au fost eliminate și a fost creată o singură frontieră externă unde controalele se desfășoară conform unui set de reguli clare.

III. Scurt istoric al spațiului Schengen

- la începutul anilor 80 a demarat, la nivel european, o discuție în legătură cu importanța termenului libertate de mișcare
- 1985 încheierea acordului între Germania, Franța, Țările de Jos, Belgia și Luxemburg
- 19 iunie 1990 semnarea Convenției de Aplicare a Acordului Schengen (CAAS)
- 1995 data intrării în vigoare a CAAS

IV. State membre Schengen

Franța, Belgia, Germania, Luxemburg, Olanda, Portugalia, Spania, Austria, Italia, Grecia, Danemarca, Finlanda, Islanda, Norvegia, Cehia, Estonia, Letonia, Lituania, Malta, Polonia, Slovacia, Slovenia, Suedia, Ungaria, Elveția.

V. Viitoare state membre ale Acordului Schengen

Cipru, Liechtenstein, Bulgaria, România

VI. Beneficii aduse de aderarea la spațiul Schengen

- Ridicarea controalelor între frontierele interne ale statelor membre Schengen
- Libertatea de mișcare a cetățenilor statelor membre
- Set de măsuri compensatorii care să diminueze impactul negativ al eliminării controalelor la frontierele interne

Pentru mai multe informații privind spațiul Schengen, vă rugăm vizitați site-ul Schengen România www.schengen.mai.gov.ro.

DEFINIȚII

date cu caracter personal - orice informații referitoare la o persoană fizică identificată sau identificabilă; o persoană identificabilă este acea persoană care poate fi identificată, direct sau indirect, în mod particular prin referire la un număr de identificare ori la unul sau la mai mulți factori specifici identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

prelucrarea datelor cu caracter personal - orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea către terți prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

operator - orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care stabilește scopul și mijloacele de prelucrare a datelor cu caracter personal; dacă scopul și mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau în baza unui act normativ, operator este persoana fizică sau juridică, de drept public ori de drept privat, care este desemnată ca operator prin acel act normativ sau în baza aceluși act normativ;

SINS - Sistemul Informatic Național de Semnalări, compatibil SIS II, care conține semnalările de interes național și de interes Schengen emise de către autoritățile naționale competente;

semnalări – set de date introduse în SINS referitoare la persoane sau bunuri identificate ori identificabile, care trebuie supuse unor măsuri dispuse de o autoritate competentă, în condițiile legii, în vederea realizării unui interes public, al respectării regimului liberei circulații a persoanelor și bunurilor sau, după caz, al asigurării ordinii și siguranței publice și al prevenirii unor amenințări la adresa securității naționale;

semnalare de interes național – o semnalare transmisă de o autoritate națională competentă din sistemul informatic propriu în SINS.

semnalare de interes Schengen – semnalare introdusă în SINS și transmisă la SIS II.

autorități naționale competente - autorități cu atribuții privind furnizarea semnalărilor în SINS respectiv SIS II și/sau consultarea semnalărilor conținute în N.SIS II, stabilite prin hotărâre de guvern în 60 de zile de la intrarea în vigoare a prezentei legi;

Sistemul Informatic Schengen (SIS) – sistemul informatic comun care permite autorităților competente din statele membre să coopereze în vederea menținerii ordinii publice și securității naționale pe teritoriile statelor membre, folosind informații comunicate prin intermediul acestui sistem;

SIS II - SIS de a doua generație compus din SIS II central, un sistem național N.SIS II în fiecare dintre statele membre și o infrastructură de comunicații care asigură conectarea N.SIS II la SIS II central;

N.SIS II – componenta națională SIS II a României formată din Sistemul Informatic Național de Semnalări și copia națională a SIS II;

copia națională a SIS II – copia completă sau parțială a bazei de date a SIS II, accesibilă pentru efectuarea de căutări efectuate pe teritoriul fiecărui stat membru; SIS II central asigură actualizarea automată a copiei naționale a SIS II, sincronizarea și consistența dintre copia națională și baza de date a SIS II, precum și inițializarea și restabilirea acesteia.