

PRELUCRAREA DATELOR PERSONALE ÎN SIS ȘI EXERCITAREA DREPTURILOR PERSOANELOR VIZATE

Spațiul Schengen reprezintă o zonă întinsă de pe continentul european în care au fost eliminate controalele la frontierele interne comune. Țările participante aplică norme comune privind controalele la frontierele externe ale spațiului Schengen, precum și în ceea ce privește acordarea vizelor și cooperarea în materie penală între serviciile polițienești și judiciare.

Sistemul de Informații Schengen (generația a doua – **SIS II**) stă la baza cooperării din spațiul Schengen. Cu ajutorul acestui sistem de informații, autoritățile de control la frontierele naționale, autoritățile vamale și autoritățile polițienești (însărcinate cu efectuarea verificărilor atât la frontierele externe, cât și în interiorul spațiului Schengen) pot transmite **alerte** cu privire la persoanele căutate sau dispărute, precum și cu privire la obiecte. Astfel, SIS II preia rolul important de a compensa desființarea controalelor la frontierele interne și facilitează libera circulație a persoanelor în spațiul Schengen.

Numai autoritățile naționale de aplicare a legii, autoritățile judiciare și autoritățile administrative au acces la SIS II. Aceste autorități pot accesa datele din SIS II de care au nevoie, strict în scopul îndeplinirii sarcinilor lor. Agențiile europene EUROPOL și EUROJUST au drepturi de acces limitate, pentru efectuarea anumitor tipuri de interogări.

SIS II este compus dintr-un sistem central, secțiuni naționale și o infrastructură de comunicații între sistemul central și secțiunile naționale. Toate sistemele naționale sunt conectate online cu sistemul central, localizat la Strasbourg.

În România s-a înființat **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.

Ministerul Afacerilor Interne, 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.

La nivelul **Inspectoratului General al Poliției Române (I.G.P.R.)** funcționează **Centrul de Cooperare Polițienească Internațională (C.C.P.I.)**, care constituie autoritatea națională centrală în domeniul cooperării polițienești internaționale. La C.C.P.I., **Biroul SIRENE** are rol esențial în funcționarea SIS. SIRENE reprezintă practic interfața umană a SIS, este **unicul punct în contactul cu celelalte state membre și asociate**. Biroul SIRENE are ca principal rol specific responsabilitatea furnizării de informații în timp real, cu posibilitatea completării informației cu date suplimentare, în cel mai scurt timp. Biroul SIRENE lucrează în regim de dispecerat, disponibil 24/7, pentru a asigura continuitatea fluxului de informații între birourile naționale echivalente. SIS fiind un **sistem hit/no-hit, semnalările sunt succinte**. Începând de la introducere și până la descoperire, **informațiile suplimentare necesare** (alte date ce pot fi solicitate de utilizatorii SIS în plus față de datele oferite

inițial de sistem, în scopul investigațiilor specifice) sunt primite/transmise de către Biroul SIRENE sub formă de formulare electronice standardizate.

PRELUCRAREA DATELOR PERSONALE ÎN SIS

Datele cu caracter personal sunt prelucrate în SIS, de la introducerea unei alerte privitor la persoana fizică și până la ștergerea acesteia din sistem, timp în care datele acesteia pot să fie consultate (de exemplu, când persoana trece frontiera externă sau este oprită pe teritoriul țării de către organele de poliție pentru o verificare polițienească) sau transmise către beneficiar (când sunt solicitate informații suplimentare).

CATEGORII DE DATE PRELUCRATE ÎN SIS

Tipurile de date care pot fi prelucrate în SIS sunt indicate în:

a) **Regulamentul (UE) 2018/1860** al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind utilizarea **Sistemului de informații Schengen pentru returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală**, denumit în continuare **Regulamentul SIS returnare**;

b) **Regulamentul (UE) 2018/1861** al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea **Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere**, de modificare a Convenției de punere în aplicare a Acordului Schengen și de modificare și abrogare a Regulamentului (CE) nr. 1987/2006, cu modificările și completările ulterioare, denumit în continuare **Regulamentul SIS verificări la frontiere**;

c) **Regulamentul (UE) 2018/1862** al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea **Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală**, de modificare și de abrogare a Deciziei 2007/533/JAI a Consiliului și de abrogare a Regulamentului (CE) nr.1986/2006 al Parlamentului European și al Consiliului și a Deciziei 2010/261/UE a Comisiei, cu modificările și completările ulterioare, denumit în continuare **Regulamentul SIS cooperare**.

SIS conține doar categoriile de date care sunt furnizate de fiecare stat membru și asociat și care sunt necesare îndeplinirii sarcinilor ce le revin (art. 4 din Regulamentul nr. 2018/1860 și art. 20 din Regulamentele nr. 2018/1861 și 2018/1862).

Regulamentul (UE) 2018/1860

Articolul 4 (1) **O semnalare privind returnarea introdusă în SIS** în conformitate cu articolul 3 din prezentul regulament **conține doar următoarele date**:

(a) numele de familie; (b) prenumele; (c) numele la naștere; (d) numele folosite anterior și pseudonimele; (e) locul nașterii; (f) data nașterii; (g) genul; (h) orice cetățenie deținută; (i) dacă persoana în cauză: (i) este înarmată; (ii) este violentă; (iii) s-a sustras sau a evadat; (iv) prezintă un risc de sinucidere; (v) reprezintă o amenințare pentru sănătatea publică; sau (vi) este implicată într-o activitate de tipul celor menționate la articolele 3-14 din Directiva (UE) 2017/541; (j) motivul semnalării; (k) autoritatea care a creat semnalarea; (l) o trimitere la decizia care a generat semnalarea; (m) acțiunea de urmat în cazul unui rezultat pozitiv; (n) legăturile cu alte semnalări în temeiul articolului 48 din Regulamentul (UE) 2018/1861; (o) dacă decizia de returnare este emisă în legătură cu un

resortisant al unei țări terțe care reprezintă o amenințare la adresa ordinii publice, pentru siguranța publică sau pentru securitatea națională; (p) tipul infracțiunii; (q) categoria documentelor de identificare ale persoanei; (r) țara care a eliberat documentele de identificare ale persoanei; (s) numărul (numerele) documentelor de identificare ale persoanei; (t) data eliberării documentelor de identificare ale persoanei; (u) fotografii și imagini faciale; (v) date dactiloscopice; (w) o copie a documentelor de identificare, color ori de câte ori este posibil; (x) ultima zi a perioadei pentru plecarea voluntară, dacă a fost acordată; (y) dacă decizia de returnare a fost suspendată sau dacă punerea în aplicare a deciziei a fost amânată, inclusiv ca rezultat al introducerii unei căi de atac; (z) dacă decizia de returnare este însoțită de o interdicție de intrare ce constituie baza unei semnalări privind refuzul intrării și al șederii în temeiul articolului 24 alineatul (1) litera (b) din Regulamentul (UE) 2018/1861.

(2) **Setul minim de date necesare** pentru a introduce o semnalare în SIS este alcătuit din datele menționate la alineatul (1) literele (a), (f), (j), (l), (m), (x) și (z). **Restul** datelor enumerate la alineatul respectiv sunt, de asemenea, înregistrate în SIS, **dacă sunt disponibile**.

Regulamentul (UE) 2018/1861

Articolul 20 (2) **Orice semnalare în SIS care include informații privind persoane conține numai următoarele date:**

(a) numele de familie; (b) prenumele; (c) numele la naștere; (d) numele folosite anterior și pseudonimul; (e) orice caracteristică fizică specifică, obiectivă și inalterabilă; (f) locul nașterii; (g) data nașterii; (h) genul; (i) orice cetățenii deținute; (j) dacă persoana în cauză: (i) este înarmată; (ii) este violentă; (iii) s-a sustras sau a evadat; (iv) prezintă un risc de sinucidere; (v) reprezintă o amenințare pentru sănătatea publică; sau (vi) este implicată într-o activitate menționată la articolele 3-14 din Directiva (UE) 2017/541; (k) motivul semnalării; (l) autoritatea care a creat semnalarea; (m) o trimitere la decizia care a generat semnalarea; (n) acțiunea de urmat în cazul unui rezultat pozitiv; (o) legăturile cu alte semnalări în temeiul articolului 48; (p) dacă persoana vizată este membru de familie al unui cetățean al Uniunii sau o altă persoană care beneficiază de dreptul de liberă circulație, astfel cum se menționează la articolul 26; (q) dacă decizia de refuz al intrării și al șederii se bazează pe: (i) o condamnare anterioară, astfel cum se menționează la articolul 24 alineatul (2) litera (a); (ii) o amenințare gravă pentru securitate, astfel cum se menționează la articolul 24 alineatul (2) litera (b); (iii) eludarea dreptului Uniunii sau a dreptului intern referitor la intrare și la ședere, astfel cum se menționează la articolul 24 alineatul (2) litera (c); (iv) o interdicție de intrare, astfel cum se menționează la articolul 24 alineatul (1) litera (b); sau (v) o măsură restrictivă, astfel cum se menționează la articolul 25; (r) tipul de infracțiune; (s) categoria documentelor de identificare ale persoanei; (t) țara care a eliberat documentele de identificare ale persoanei; (u) numărul (numerele) documentelor de identificare ale persoanei; (v) data eliberării documentelor de identificare ale persoanei; (w) fotografii și imagini faciale; (x) date dactiloscopice; (y) o copie a documentelor de identificare, color, ori de câte ori este posibil.

Regulamentul (UE) 2018/1862

Articolul 20 (2) **Categoriile de date sunt următoarele:**

(a) informații privind persoanele cu privire la care au fost introduse semnalări;

(b) informații privind obiectele menționate la articolele 26, 32, 34, 36 și 38.

(3) **Orice semnalare în SIS care include informații privind persoane conține numai următoarele date:**

(a) numele de familie; (b) prenumele; (c) numele la naștere; (d) numele folosite anterior și pseudonimul; (e) orice caracteristică fizică specifică, obiectivă și inalterabilă; (f) locul nașterii; (g) data nașterii; (h) genul; (i) toate cetățeniile deținute; (j) dacă persoana în cauză: (i) este înarmată; (ii) este violentă; (iii) s-a sustras sau a evadat; (iv) prezintă un risc de sinucidere; (v) reprezintă o amenințare pentru sănătatea publică; sau (vi) este implicată într-o activitate menționată la articolele 3-14 din Directiva (UE) 2017/541; (k) motivul semnalării; (l) autoritatea care a creat semnalarea; (m) o trimitere la decizia care a generat semnalarea; (n) acțiunea de urmat în cazul unui rezultat pozitiv; (o) legăturile cu alte semnalări în temeiul articolului 63; (p) tipul de infracțiune; (q) numărul de înregistrare al persoanei în cauză într-un registru național; (r) pentru semnalările menționate la articolul 32 alineatul (1), o clasificare a tipului de caz; (s) categoria documentelor de identificare ale persoanei; (t) țara care a eliberat documentele de identificare ale persoanei; (u) numărul (numerele) documentelor de identificare ale persoanei; (v) data eliberării documentelor de identificare ale persoanei; (w) fotografiile și imagini faciale; (x) în conformitate cu articolul 42 alineatul (3), profilurile ADN relevante; (y) date dactiloscopice; (z) o copie a documentelor de identificare, color, ori de câte ori este posibil.

Semnalările introduse în SIS se referă la:

- persoane căutate în vederea arestării în scopul predării sau al extrădării;
- persoane dispărute sau vulnerabile care trebuie împiedicate să călătorească;
- persoane căutate în vederea participării la o procedură judiciară;
- persoane și obiecte în scopul efectuării de controale discrete, de controale prin interviu sau de controale specifice;
- obiecte căutate pentru a fi confiscate sau folosite ca probe în cadrul procedurilor penale;
- persoane necunoscute căutate în scopul identificării în temeiul dreptului intern;
- resortisanții țărilor terțe cărora li se aplică decizii de returnare emise de statele membre;
- resortisanții țărilor terțe cărora li se refuză intrarea sau șederea pe teritoriul statelor membre.

AUTORITĂȚI CU ACCES LA SIS

SIS susține activitățile:

- forțelor de poliție sau poliție de frontieră;
- autorităților judiciare și a celor responsabile pentru prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor de terorism sau a altor infracțiuni grave ori executarea pedepselor;
- autorităților în materie de vize sau de imigrări;
- autorităților vamale;
- autorităților responsabile de înmatricularea vehiculelor, emiterea documentelor, înregistrarea armelor sau a altor tipuri de obiecte.

PROTECȚIA DATELOR PERSONALE ÎN SIS

Fiecare stat membru și asociat aplică propriile norme privind secretul profesional sau alte obligații echivalente de confidențialitate pentru toate persoanele și organismele care lucrează cu date din SIS și cu informații suplimentare, în conformitate cu dreptul său intern. Prelucrarea datelor în SIS se realizează în conformitate cu regulile de protecție a datelor europene și naționale.

Datele pot fi utilizate numai în scopurile specificate în cadrul fiecărei categorii de semnalări. Datele pot fi copiate numai în scopuri tehnice și nu pot fi utilizate în scopuri administrative. Excepțiile sunt punctuale.

Înainte de a fi autorizat să prelucreze datele stocate în SIS și periodic după acordarea accesului la datele din SIS, personalul autorităților care au drept de acces la SIS beneficiază de o formare corespunzătoare inclusiv privind securitatea datelor, drepturile fundamentale (protecția datelor), normele și procedurile referitoare la prelucrarea datelor.

Orice accesare a datelor cu caracter personal și toate schimburile de date cu caracter personal din baza de date din SIS sunt înregistrate în propriul N.SIS în scopul verificării legalității căutării, al monitorizării legalității prelucrării datelor, al automonitorizării și al asigurării funcționării corespunzătoare a N.SIS, precum și a integrității și securității datelor. Înregistrările se pot utiliza numai în scopurile menționate anterior și se șterg la trei ani de la crearea. Înregistrările care includ istoricul semnalărilor se șterg la trei ani de la ștergerea semnalărilor.

DREPTURILE PERSOANELOR VIZATE DE PRELUCRAREA DATELOR PERSONALE ÎN SIS

Drepturile garantate persoanelor vizate (prevăzute la art. 19 din Regulamentul (UE) nr. 2018/1860, art. 53 din Regulamentul (UE) nr. 2018/1861 și articolul 67 din Regulamentul (UE) nr. 2018/1862) sunt:

- **dreptul de acces la datele persoanele** (persoana vizată are dreptul de a ști dacă datele sale sunt înregistrate sau nu în SIS);
- **dreptul de rectificare a datelor inexacte** (persoana vizată are dreptul de a solicita corectarea datelor eronate din SIS);
- **dreptul de ștergere a datelor stocate ilegal** în sistem (persoana vizată are dreptul de a solicita ștergerea datelor, dacă acest lucru este permis de lege).

EXERCITAREA DREPTURILOR PERSOANELOR VIZATE

Drepturile de acces, rectificare și ștergere a datelor în contextul prelucrării datelor cu caracter personal în SIS se exercită, după caz, conform:

- **Regulamentului (UE) nr. 2016/679** al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
- **Legii nr. 363/2018** privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date.

Pentru exercitarea drepturilor (dreptul de acces, dreptul de rectificare, dreptul de ștergere), **persoana vizată poate:**

- transmite/depune o cerere la **sediul I.G.P.R.** din București, sector 5, strada Mihai Vodă, nr. 6, cod poștal 030167;

- transmite o cerere în format electronic, la **adresa de e-mail I.G.P.R.:** ccpi@mai.gov.ro

Cererile depuse/transmise la **orice operator de date din cadrul Ministerului Afacerilor Interne** (site-ul I.G.P.F. - www.politiadefrontiera.ro, site-ul I.G.I. - igi.mai.gov.ro sau altele) vor fi transmise Biroului SIRENE din cadrul I.G.P.R., în termen de 5 zile de la data primirii acestora,

conform Legii nr. 141/2010 privind înființarea, organizarea și funcționarea Sistemului Informatic Național de Semnalări și participarea României la Sistemul de Informații Schengen, republicată (acest act normativ urmează să fie abrogat de către o lege care stabilește măsurile premergătoare, condițiile și procedurile referitoare la introducerea și prelucrarea în Sistemul Informatic Național de Semnalări, a semnalărilor de interes național, în aplicarea la nivel național a anumitor prevederi cuprinse în Regulamentele Europene nr. 2018/1860, 2018/1861 și 2018/1862).

Modele de cereri se regăsesc în partea de jos a paginii curente.

Cererile de rectificare și/sau ștergere trebuie să cuprindă în mod obligatoriu datele cu caracter personal a căror rectificare și/sau ștergere se solicită.

Cererile trebuie să fie semnate de persoana ale cărei date au fost prelucrate și sunt considerate valide doar în situația se face dovada identității (cu o copie a unui document de identitate). În cazul în care persoana vizată este reprezentată de avocat, cererea trebuie să fie semnată atât de către persoana vizată cât și de avocat, trebuie să fie însoțită de împuternicirea avocațială, precum și de o copie a unui document de identitate al persoanei vizate.

SOLUȚIONAREA CERERILOR

Biroul SIRENE, din cadrul I.G.P.R., este singurul abilitat din România să răspundă acestor cereri. Acesta este obligat să comunice persoanei vizate informații privind acțiunile întreprinse în urma unei cereri depuse în temeiul art. 15, 16, 17 din Regulamentul (UE) 2016/679, respectiv art. 16 și 18 alin. 1, 3 din Legea nr. 363/2018, **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, și cât mai curând posibil, dar nu mai târziu de 90 de zile de la data primirii cererii, în cazul exercitării dreptului de rectificare și ștergere a datelor personale** (conform art. 62, alin. 2 din Legea nr. 141/2010).

În cazul în care persoana vizată introduce **cererea în format electronic**, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.

Orice comunicare și orice măsuri luate sunt oferite de I.G.P.R. gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, I.G.P.R. poate:

- să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate sau
- să refuze să dea curs cererii.

EXCEPȚIILE PRIVIND EXERCITAREA DREPTURILOR (art. 19 din Regulamentul (UE) 2018/1860, art. 53 din Regulamentul (UE) 2018/1861 și articolul 67 din Regulamentul (UE) 2018/1862)

Un stat membru ia **decizia de a nu furniza, integral sau parțial, informații persoanei vizate**, în conformitate cu dreptul intern, în măsura în care și atât timp cât o astfel de restricționare parțială sau integrală constituie o măsură necesară și proporționată într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei vizate în cauză, pentru: (a) a nu obstrucționa cercetările, investigațiile sau procedurile oficiale ori judiciare; (b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor; (c) a proteja siguranța publică; (d) a proteja securitatea națională; sau (e) a proteja drepturile și libertățile celorlalți.

Statul membru informează persoana vizată despre posibilitatea de a depune o plângere la autoritatea de supraveghere sau de a introduce o cale de atac judiciară.

CĂI DE ATAC (art. 19 din Regulamentul (UE) 2018/1860, art. 54 din Regulamentul (UE) 2018/1861 și articolul 68 din Regulamentul (UE) 2018/1862)

Fără a aduce atingere dispozițiilor privind căile de atac din Regulamentul (UE) 2016/79 și din Directiva (UE) 2016/680, orice persoană poate introduce o **acțiune în fața oricărei autorități competente, inclusiv a unei instanțe judecătorești**, în temeiul dreptului oricărui stat membru, pentru accesul, rectificarea, ștergerea, obținerea informațiilor ori pentru obținerea de despăgubiri în legătură cu o semnalare care o privește.

Dreptul de a depune o plângere la o autoritate de supraveghere (articolul 77 din Regulamentul UE 2016/679, art. 57 din Legea nr. 363/2018)

Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă Regulamentul UE 2016/679 sau Legea nr. 363/2018.

Coordonatele de contact ale Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (A.N.S.P.D.C.P.):

Sediul: B-dul G-ral Gheorghe Magheru 28-30, sector 1, cod poștal 010336, București

Telefon: 031.805.92.11; Fax: 031.805.96.02

Internet: www.dataprotection.ro E-mail: anspdcpc@dataprotection.ro

Pentru a depune o plângere la A.N.S.P.D.C.P. [click aici](#)

Dreptul la o cale de atac judiciară eficientă împotriva unui operator (Articolul 79 din Regulamentul UE 2016/679, art. 58 din Legea nr. 363/2018)

Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere în temeiul articolului 77, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază în temeiul Regulamentului UE 2016/679 sau Legii nr. 363/2018 au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal fără a se respecta cele două acte normative.

MODELE CERERI PENTRU EXERCITAREA DREPTURILOR

CERERE PENTRU EXERCITAREA DREPTULUI DE ACCES

Către

INSPECTORATUL GENERAL AL POLIȚIEI ROMÂNE
București, strada Mihai Vodă, nr. 6, sector 5

Subsemnatul/a (numele și prenumele), cu domiciliul/reședința în str. nr. bl. sc. ap., județul/sectorul..... CNP..... telefon , adresa de e-mail (opțional)....., în temeiul art. 16 din Legea nr. 363/2018, vă rog să-mi comunicați dacă datele mele cu caracter personal au fost prelucrate de către instituția dumneavoastră, în perioada/data, prin intermediul Sistemului Informatic Shengen.

(opțional) Cererea este depusă prin reprezentant(se vor menționa datele de identificare ale acestuia), sens în care depun împuternicirea avocațială/procura notarială de reprezentare (se menționează varianta corespunzătoare).

Doresc ca informațiile să îmi fie comunicate la adresa de domiciliu/reședință sau pe cale electronică, la adresa de e-mail:

În baza art. 12, alin. 10 din Legea nr. 363/2018, pentru verificarea identității mele ca persoană vizată care formulează cererea de acces la datele sale cu caracter personal, anexez copie după documentul de identitate.

Declar pe propria răspundere că datele completate în prezenta cerere sunt reale și corecte.

Data
Semnătura

CERERE PENTRU EXERCITAREA DREPTULUI DE RECTIFICARE

Către

INSPECTORATUL GENERAL AL POLIȚIEI ROMÂNE
București, strada Mihai Vodă, nr. 6, sector 5

Subsemnatul/a (numele și prenumele), cu domiciliul/reședința în str. nr. bl. sc. ap., județul/sectorul..... CNP..... telefon , adresa de e-mail (opțional)....., în temeiul art. 18, alin. 1 din Legea nr. 363/2018, vă rog să dispuneți măsurile legale pentru rectificarea următoarelor date cu caracter personal care mă privesc (se enumeră datele respective), pentru următoarele motive: (se menționează motivele).

(opțional) Cererea este depusă prin reprezentant(se vor menționa datele de identificare ale acestuia), sens în care depun împuternicirea avocațială/procura notarială de reprezentare (se menționează varianta corespunzătoare).

Doresc ca informațiile privind modul de soluționare a prezentei cereri să îmi fie comunicate la adresa de domiciliu/reședință sau pe cale electronică, la adresa de e-mail:

În baza art. 12, alin. 10 din Legea nr. 363/2018, pentru verificarea identității mele ca persoană vizată care formulează cererea de acces la datele sale cu caracter personal, anexez copie după documentul de identitate.

Declar pe propria răspundere că datele completate în prezenta cerere sunt reale și corecte.

Data
Semnătura

CERERE PENTRU EXERCITAREA DREPTULUI DE ȘTERGERE A DATELOR

Către

INSPECTORATUL GENERAL AL POLIȚIEI ROMÂNE
București, strada Mihai Vodă, nr. 6, sector 5

Subsemnatul/a (numele și prenumele), cu domiciliul/reședința în str. nr. bl. sc. ap., județul/sectorul..... CNP..... telefon , adresa de e-mail (opțional)....., în temeiul art. 18, alin. 3 din Legea nr. 363/2018, vă rog să dispuneți măsurile legale pentru ștergerea următoarelor date cu caracter personal care mă privesc (se enumeră datele respective), pentru următoarele motive: nu mai sunt necesare pentru îndeplinirea scopului pentru care au fost colectate sau prelucrate/îmi retrag consimțământul/au fost prelucrate ilegal/respectarea unei obligații legale care vă revine (se menționează varianta corespunzătoare). (opțional) Cererea este depusă prin reprezentant(se vor menționa datele de identificare ale acestuia), sens în care depun împuternicirea avocațială/procura notarială de reprezentare (se menționează varianta corespunzătoare).

Doresc ca informațiile privind modul de soluționare a prezentei cereri să îmi fie comunicate la adresa de domiciliu/reședință sau pe cale electronică, la adresa de e-mail:

În baza art. 12, alin. 10 din Legea nr. 363/2018, pentru verificarea identității mele ca persoană vizată care formulează cererea de acces la datele sale cu caracter personal, anexez copie după documentul de identitate.

Declar pe propria răspundere că datele completate în prezenta cerere sunt reale și corecte.

Data _____ Semnătura _____

* Durata de completare a unei cereri pentru exercitarea drepturilor poate varia în funcție de informațiile suplimentare pe care persoana vizată dorește să le menționeze. Informațiile standard ale cererii pot fi completate în aproximativ 2 minute.

DATELE DE CONTACT ALE RESPONSABILULUI CU PROTECȚIA DATELOR

La nivelul IGPR funcționează Compartimentul Protecția Datelor cu Caracter Personal.

Sediul: București, sector 2, Șoseaua Ștefan cel Mare, nr. 13-15

Adresa e-mail: cpdcp@politiaromana.ro ; Telefon: 021/208.25.25 (centrala), interior 26559.

Actualizat la data de 22.08.2022