2025

ROMÂNIA
MINISTERUL AFACERILOR INTERNE
INSPECTORATUL GENERAL AL POLIȚIEI DE FRONTIERĂ

NOTĂ DE INFORMARE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL DE CĂTRE POLIȚIA DE FRONTIERĂ ROMÂNĂ PRIN SISTEMUL DE INFORMAȚII PRIVIND VIZELE

Această notă de informare explică modul în care Poliția de Frontieră Română colectează, utilizează și protejează datele cu caracter personal, conform Regulamentului nr. 767/2008 (Regulamentul VIS) și ale Legii nr. 271/2010 (SNIV). Veți găsi detalii despre drepturile dumneavoastră privind datele personale, motivele și temeiurile prelucrării acestora, precum și măsurile de protecție aplicate.

Cuprins

NOTĂ DE INFORMARE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL DE CĂTRE POLIȚIA DE FRONTIERĂ ROMÂNĂ PRIN SISTEMUL DE INFORMAȚII PRIVIND VIZELE 0

1. INFORMARE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL DE CĂTRE POLIȚIA DE FRONTIERĂ ROMÂNĂ PRIN VIS/SNIV 2

1.1. Identitatea operatorilor de date din cadrul Poliției de Frontieră Române 2

1.2. Informații generale despre Inspectoratul General al Poliției de Frontieră Române 2

2.TEMEIUL LEGAL AL PRELUCRĂRII DATELOR 2

3. SISTEMUL DE INFORMAȚII PRIVIND VIZELE (VIS) 4

3.1. Ce este VIS? 4

3.2. Care este scopul VIS? 4

3.3. Ce date sunt stocate în VIS? 4

3.4. Ce state utilizează VIS și cine il gestionează? 5

3.5. Cine poate accesa VIS? 5

3.6. Cum sunt protejate datele mele în VIS? 6

4. SISTEMUL NAȚIONAL DE INFORMAȚII PRIVIND VIZELE (SNIV) 6

4.1. Ce este SNIV? 6

4.2. Drepturile persoanelor fizice 7

4.3. Dreptul de a depune o plângere la autoritatea pentru protecția datelor 8

4.4. Dreptul la o cale de atac judiciară 8

5. RESTRICȚII 8

5.1. Restricții și limitări privind exercitarea drepturilor persoanelor vizate 8

6. AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL (A.N.S.P.D.C.P.) 9

7. DEFINIȚII 12

8. PRINCIPII ȘI LEGALITATEA PRELUCRĂRII DATELOR CU CARACTER PERSONAL 13

8.1. Principii legate de prelucrarea datelor cu caracter personal: 13

8.2. Legalitatea prelucrării: 13

9. DATE DE CONTACT 14

1. INFORMARE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL DE CĂTRE POLIȚIA DE FRONTIERĂ ROMÂNĂ PRIN VIS/SNIV

1.1. Identitatea operatorilor de date din cadrul Poliției de Frontieră Române

Prezenta informare vizează furnizarea unor informații cu caracter general cu privire la prelucrarea datelor dumneavoastră personale și la drepturile pe care le aveți în conformitate cu Regulamentul (CE) nr. 767/2008 și Legea nr. 271/2010

În conformitate cu legislația națională și europeană în vigoare, Inspectoratul General al Poliției de Frontieră, în calitatea sa de operator de date cu caracter personal, este preocupat în mod constant de asigurarea unei protecții a persoanelor cu privire la prelucrările de date cu caracter personal pe care le efectuează conform cadrului legal în vigoare.

Poliţia de Frontieră Română (PFR) face parte din Ministerul Afacerilor Interne (MAI) şi este instituţia specializată a statului care exercită atribuţiile ce îi revin cu privire la supravegherea şi controlul trecerii frontierei de stat, prevenirea şi combaterea migraţiei ilegale şi a faptelor specifice criminalităţii transfrontaliere săvârşite în zona de competenţă, respectarea regimului juridic al frontierei de stat, paşapoartelor şi străinilor, asigurarea intereselor statului român pe Dunărea interioară, inclusiv braţul Măcin şi canalul Sulina situate în afara zonei de frontieră, în zona contiguă şi în zona economică exclusivă, respectarea ordinii şi liniştii publice în zona de competenţă, în condiţiile legii.

În conformitate cu prevederile **O.U.G. nr. 104/2001** *privind organizarea și funcționarea Poliției de Frontieră Române*, cu modificările și completările ulterioare, activitatea PFR constituie serviciu public şi se desfăşoară în interesul persoanei, al comunităţii şi în sprijinul instituţiilor statului, exclusiv pe baza şi în executarea legii.

Poliția de Frontieră Română are în structura sa unitatea centrală, unități teritoriale și unități de învățământ care prelucrează date cu caracter personal. Astfel, în cadrul Poliţiei de Frontieră Române sunt operatori de date distincți: Inspectoratul General al Poliției de Frontieră Române (I.G.P.F.), Inspectorate Teritoriale ale Poliției de Frontieră (I.T.P.F. Iași, I.T.P.F. Giurgiu, I.T.P.F. Timișoara, I.T.P.F. Oradea și I.T.P.F. Sighetu Marmației) și Garda de Coastă Constanța.

1.2. Informații generale despre Inspectoratul General al Poliției de Frontieră Române

Inspectoratul General al Poliţiei de Frontieră (IGPF) este unitatea centrală a PFR, cu personalitate juridică şi competenţă teritorială pentru întreaga zona de responsabilitate a poliţiei de frontieră, care exercită conducerea şi răspunde de întreaga activitate a poliţiei de frontieră, desfăşoară activităţi de investigare şi cercetare a infracţiunilor deosebit de grave circumscrise crimei organizate, migraţiei ilegale şi criminalităţii transfrontaliere comise în zona de competenţă teritorială a PFR, precum şi orice alte atribuţii date în competenţa sa prin lege.

IGPF este operator de date cu caracter personal, în conformitate cu art. 4 pct. 7 din **Regulamentul (UE) 2016/679** *al Parlamentului European și al Consiliului 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 (RGPD)*.

*2.*TEMEIUL LEGAL AL PRELUCRĂRII DATELOR

- Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului din 9 martie 2016 *cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen);*

- Regulamentul (UE) 2017/458 al Parlamentului European și al Consiliului din 15 martie 2017 *de modificare a Regulamentului (UE) 2016/399 în ceea ce privește consolidarea verificărilor prin consultarea bazelor de date relevante la frontierele externe;*
- Convenția de Aplicare a Acordului de la Schengen din 14.06.1985, semnată la Schengen la 19.06.1990, *privind eliminarea treptată a controalelor la frontierele comune, cu modificările și completările ulterioare;*
- REGULAMENTUL (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 *privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE în domeniul frontierelor și al vizelor;*
- **Regulamentul (UE) 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);*
- **Directiva (UE) 2016/680** a Parlamentului European și a Consiliului din 27 aprilie 2016 *privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului;*
- Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS);
- Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului din 13 iulie 2009 privind instituirea unui Cod comunitar de vize (Codul de vize);
- Regulamentul (UE) 2018/1806 al Parlamentului European și al Consiliului din 14 noiembrie 2018 de stabilire a listei țărilor terțe ai căror resortisanți trebuie să dețină viză pentru trecerea frontierelor externe și a listei țărilor terțe ai căror resortisanți sunt exonerați de această obligație;
- Regulamentul (UE) 2017/1370 al Parlamentului European și al Consiliului din 4 iulie 2017 de modificare a Regulamentului (CE) nr. 1683/95 al Consiliului de instituire a unui model uniform de viză;
- Regulamentul (UE) 2021/1134 al Parlamentului European și al Consiliului din 7 iulie 2021 de modificare a Regulamentelor (CE) nr. 767/2008, (CE) nr. 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 și (UE) 2019/1896 ale Parlamentului European și ale Consiliului și de abrogare a Deciziilor 2004/512/CE și 2008/633/JAI ale Consiliului, în scopul reformării Sistemului de informații privind vizele;
- Regulamentul (UE) 2021/1133 al Parlamentului European și al Consiliului din 7 iulie 2021 de modificare a Regulamentelor (UE) nr. 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 și (UE) 2019/818 în ceea ce privește stabilirea condițiilor de acces la celelalte sisteme de informații ale UE în scopuri legate de Sistemul de informații privind vizele;
- Legea nr. 271/2010 pentru înființarea, organizarea şi funcționarea Sistemului naţional de informaţii privind vizele şi participarea României la Sistemul de informaţii privind vizele.
- O.U.G. nr. 104/2001 *privind organizarea și funcționarea Poliției de Frontieră Române, cu modificările și completările ulterioare, republicată;*
- O.U.G. nr. 105/2001 *privind frontiera de stat a României;*
- H.G. nr. 445/2002 *pentru aprobarea Normelor metodologice de aplicare a O.U.G. nr. 105/2001 privind frontiera de stat a României;*
- O.U.G. nr. 194/2002 *privind regimul străinilor în România;*
- O.U.G. nr. 103/2006 *privind unele măsuri pentru facilitarea cooperării polițienești internaționale, cu modificările și completările ulterioare, republicată;*

- O.U.G. nr. 102/2005 *privind libera circulație pe teritoriul României a cetățenilor statelor membre ale Uniunii Europene, Spațiul Economic European și al cetățenilor Confederației Elvețiene;*
- Lege nr. 190/2018 *privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)*;
- Lege nr. 363/2018 *privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date*;
- Lege nr. 102/2005 *privind înființarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată, cu modificările și completările ulterioare;*

3. SISTEMUL DE INFORMAȚII PRIVIND VIZELE (VIS)

3.1. Ce este VIS?

Sistemul de informații privind vizele (VIS) permite statelor Schengen să realizeze un schimb de date privind vizele. Acesta constă într-un sistem informatic central și o infrastructură de comunicații care leagă acest sistem central de sistemele naționale. VIS conectează consulatele din statele terțe și toate punctele de trecere a frontierelor externe ale statelor Schengen. Acesta prelucrează date și decizii referitoare la cererile de viză de scurtă ședere pentru a vizita sau a tranzita spațiul Schengen. Sistemul poate efectua comparații biometrice, în principal ale amprentelor digitale, în scopul identificării și verificării.

3.2. Care este scopul VIS?

Facilitarea controalelor și eliberarea vizelor: VIS permite polițiștilor de frontieră să verifice dacă o persoană care prezintă o viză este titularul de drept al acesteia și să identifice persoanele găsite pe teritoriul Schengen fără documente sau cu documente frauduloase. Utilizarea datelor biometrice pentru a confirma identitatea unui titular de viză permite verificări mai rapide, mai precise și mai sigure. Sistemul facilitează, de asemenea, procesul de eliberare a vizelor.

Combaterea abuzurilor: Deși marea majoritate a titularilor de viză respectă reglementările în vigoare, pot avea loc și abuzuri. De exemplu, VIS contribuie la combaterea și prevenirea comportamentelor frauduloase, cum ar fi „***visa shopping***” (adică practica de a depune noi cereri de viză în alte state membre ale UE atunci când o primă cerere a fost respinsă).

Protejarea călătorilor: Tehnologia biometrică permite detectarea călătorilor care utilizează documentele de călătorie ale unei alte persoane și protejează călătorii împotriva furtului de identitate.

Asistență în ceea ce privește cererile de azil: VIS facilitează stabilirea statului UE responsabil de examinarea unei cereri de azil și examinarea unor astfel de cereri.

Consolidarea securității: VIS contribuie la prevenirea, depistarea și investigarea infracțiunilor de terorism și a altor infracțiuni grave.

3.3. Ce date sunt stocate în VIS?

Se colectează 10 amprente digitale și o fotografie digitală de la persoanele care solicită o viză. Aceste date biometrice, împreună cu datele furnizate în formularul de cerere de viză, sunt înregistrate într-o bază de date centrală securizată.

Nu sunt necesare scanări ale celor 10 degete la copiii sub vârsta de 12 ani sau la persoanele care nu pot efectua scanări ale degetului. Persoanele care călătoresc frecvent în spațiul Schengen nu trebuie să efectueze noi scanări ale degetelor de fiecare dată când solicită o nouă viză. Odată ce scanările degetelor sunt stocate în VIS, acestea pot fi reutilizate pentru alte cereri de viză pe o perioadă de 5 ani.

La frontierele externe ale spațiului Schengen, scanările degetului titularului vizei pot fi comparate cu cele din baza de date. O neconcordanță nu înseamnă că intrarea va fi refuzată în mod automat, ci va conduce doar la verificări suplimentare ale identității călătorului.

În conformitate cu Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 *privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS)* datele sunt stocate in baza de date VIS dacă:

- datele sunt introduse la depunerea cererii (art. 9)
- datele sunt adăugate în cazul eliberării unei vize (art. 10)
- datele sunt adăugate în cazul suspendării examinării cererii de viză (art. 11)
- datele sunt adăugate în cazul refuzului unei vize (art. 12)
- datele sunt adăugate în cazul anulării sau al retragerii unei vize sau al reducerii duratei sale de valabilitate (art. 13)
- datele sunt adăugate în cazul prelungirii unei vize.

Datele stocate în baza de date se referă la identitatea autorității care examinează cererea, elemente privind procesul de solicitare în sine (precum data, tipul vizei), numele solicitantului, scopul călătoriei, durata șederii, o fotografie și amprenta digitală.

Datele sunt păstrate în VIS pentru o perioadă de până la 5 ani. Această perioadă de păstrare începe de la data expirării vizei emise, de la data la care este luată o decizie negativă sau de la data la care este luată o decizie de modificare a unei vize emise.

Datele sunt introduse în VIS de către autoritățile naționale. Autoritățile care au acces la VIS trebuie să se asigure că utilizarea acestuia este limitată la ceea ce este necesar, adecvat și proporțional pentru îndeplinirea sarcinilor. În plus, acestea trebuie să se asigure că, la utilizarea VIS, solicitanții și titularii de vize nu sunt discriminați și că demnitatea și integritatea lor umană sunt respectate.

3.4. Ce state utilizează VIS şi cine il gestionează?

Ca instrument Schengen, VIS se aplică tuturor statelor Schengen. Agenția UE pentru sisteme informatice la scară largă, eu-LISA, este responsabilă de gestionarea operațională a VIS.

3.5. Cine poate accesa VIS?

Autoritățile competente în domeniul vizelor pot consulta VIS în scopul examinării cererilor și a deciziilor legate de acestea.

Autoritățile responsabile cu efectuarea verificărilor la frontierele externe și pe teritoriilor naționale au acces pentru a efectua căutări în VIS în scopul de a verifica identitatea persoanei, autenticitatea vizei sau dacă persoana îndeplinește cerințele pentru intrarea, șederea sau reședința pe teritoriile naționale.

Autoritățile competente în domeniul azilului au acces la VIS numai în scopul stabilirii statului UE responsabil de examinarea unei cereri de azil.

În cazuri specifice, autoritățile naționale și Europol pot solicita accesul la datele introduse în VIS în scopul prevenirii, depistării și investigării infracțiunilor de terorism și a infracțiunilor grave.

3.6. Cum sunt protejate datele mele în VIS?

Accesul la datele din VIS este limitat la personalul autorizat în îndeplinirea sarcinilor sale. Acestea trebuie să se asigure că utilizarea datelor din VIS se limitează la ceea ce este necesar, adecvat și proporțional pentru îndeplinirea sarcinilor lor.

Datele sunt păstrate în VIS timp de 5 ani. Această perioadă de păstrare începe de la data expirării vizei eliberate, de la data la care se ia o decizie negativă sau de la data la care se ia o decizie de modificare a unei vize eliberate. Orice persoană are dreptul de a fi informată cu privire la datele sale în VIS. Orice persoană poate solicita ca datele inexacte despre ea să fie corectate și datele înregistrate ilegal să fie șterse.

Fiecare stat membru al UE trebuie să asigure existența unei autorități naționale de supraveghere care să monitorizeze legalitatea prelucrării datelor cu caracter personal de către țara respectivă. Autoritatea Europeană pentru Protecția Datelor va monitoriza activitățile la nivel european.

4. SISTEMUL NAȚIONAL DE INFORMAȚII PRIVIND VIZELE (SNIV)

4.1. Ce este SNIV?

Sistemul Naţional de Informaţii privind Vizele (SNIV) este un sistem informatic înalt securizat, operaţional exclusiv în reţeaua securizată a MAE, integral compatibil cu specificaţiile Sistemului central de informaţii privind vizele – *Central Visa Information System* (C.VIS) , fiind destinat gestionării datelor şi schimbului de date privind vizele. Prin conectarea la C.VIS, autorităţile competente din SM ale spaţiului Schengen, au posibilitatea de a introduce, de a actualiza şi de a consulta aceste date, pe cale electronică.

SNIV a fost configurat de aşa natură încât să permită autorităţilor române competente să participe la acest schimb de date şi să gestioneze, la nivel naţional, cererile de vize formulate de către cetăţenii statelor terţe supuşi obligativităţii vizei de intrare în România.

Prin prelucrarea datelor solicitanţilor de vize/permise de mic trafic (PMT) în baza naţională de date aferentă, SNIV se constituie ca o componentă electronică cu acces limitat şi securizat, în care sunt prelucrate şi cuprinse date cu caracter personal introduse exclusiv în scopurile bine-determinate şi legale ale examinării cererilor de vize şi de PMT formulate de către cetăţenii străini care doresc să călătorească în România, precum şi pentru eliberarea acestor documente.

Legea nr.271/2010 (Legea SNIV) reglementează tipurile de tranzacţii ce sunt efectuate asupra datelor cu caracter personal în SNIV (cf. art.10 – 25 din Legea SNIV), în linie cu dispoziţiile Regulamentului VIS.

Specificaţiile SNIV evoluează odată cu evoluţiile specificaţiilor C.VIS, fiind asigurată compatibilizarea permanentă a celor două sisteme.

Datele cu caracter personal prelucrate prin intermediul SNIV sunt utilizate exclusiv în scopurile pentru care sunt preluate şi procesate (vize şi PMT).

Personalul Poliţiei de Frontieră Române cu atribuţii în preluarea datelor din SNIV, precum şi pentru eliberarea de vize, procesează date cu caracter personal în baza următoarelor principii:
a) legalitate, echitate și transparență - datele cu caracter personal sunt prelucrate în mod legal, echitabil și transparent față de persoana vizată;

b) limitări legate de scop – datele cu caracter personal sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale;

c) reducerea la minimum a datelor – datele cu caracter personal sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;

d) exactitate - datele cu caracter personal sunt exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere;

e) limitări legate de stocare - datele cu caracter personal sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele;

f) integritate și confidențialitate - datele cu caracter personal sunt prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare;

g) responsabilitate - operatorul este responsabil de respectarea tuturor principiilor enunţate anterior și poate demonstra această respectare.
Datele cu caracter personal prelucrate în SNIV sunt protejate în conformitate cu dispoziţiile legale în materie, fiind asigurată alinierea la principiile enunţate mai sus.

4.2. Drepturile persoanelor fizice

În conformitate cu cadrul legal aplicabil, fiecare persoană are dreptul:

- de acces la informaţiile stocate în VIS
- de rectificare a datelor inexacte sau incorecte
- de ștergere a datelor prelucrate ilegal
- de a depune o plângere la autoritatea națională pentru protecția datelor
- de a se adresa instanțelor judecătorești.

Potrivit art. 44 din Legea nr. 271/2010, cererile care privesc exercitarea drepturilor persoanei vizate în contextul prelucrării datelor cu caracter personal în Sistemul National de Informaţii privind Vize (SNIV) sau Sistemul de Informaţii privind Vizele (VIS) se adresează Centrului National de Vize, iar răspunsul va fi comunicat petentului cât mai curând posibil, dar nu mai târziu de 60 de zile de la data primirii cererii.

Termenul prevăzut mai sus se prelungește la 90 de zile, în cazul în care solicitarea se referă la date care au fost introduse de un alt stat membru.

Adresa de corespondență pentru transmiterea cererilor de exercitare a drepturilor în contextul prelucrării datelor cu caracter personal în SNIV sau în VIS:

Ministerul Afacerilor Externe prin misiunile diplomatice/oficiile consulare ale României şi Centrul Naţional de Vize
Sediul în Aleea Alexandru nr.31, Sector 1, București, cod poștal 011822
Tel.: +40 21 431 11 00; +40 21 431 15 62; +40 21 319 21 08; +40 21 319 21 25

Fax: +40 21 319 68 62
Email: dpo@mae.ro

4.3. Dreptul de a depune o plângere la autoritatea pentru protecția datelor

Legalitatea prelucrării datelor cu caracter personal în SNIV sau VIS pe teritoriul României şi transmiterea acestor date în străinătate, precum şi schimbul ori prelucrarea ulterioară a informațiilor suplimentare sunt monitorizate şi se supun controlului Autorităţii Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

Fără a aduce atingere oricăror altor 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 prevederile legale aplicabile în domeniu.

Potrivit Procedurii de soluționare a plângerilor, adoptată prin Decizia nr. 133/2018, la depunerea plângerilor este obligatorie precizarea detaliată a obiectului acestora, a demersurilor întreprinse de petiționar la nivelul operatorului reclamat sau al persoanei împuternicite reclamate, după caz, a informațiilor disponibile pentru susținerea afirmațiilor, precum şi anexarea de dovezi concludente.

Datele de contact ale Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal sunt:

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)
Bd. G-ral Gheorghe Magheru nr. 28-30
Sector 1, București, cod poștal 010336
România
Tel.: +40 31 805 92 11
Fax: +40 31 805 96 02
E-mail: anspdcp@dataprotection.ro

4.4. Dreptul la o cale de atac judiciară

Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal.

5. RESTRICȚII

5.1. Restricții și limitări privind exercitarea drepturilor persoanelor vizate

Restricțiile privind exercitarea drepturilor persoanelor vizate sunt prevăzute la art. 23 din Regulamentul (UE) 2016/679. Dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la articolele 5, 12-22 și 34 din GDPR, în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la articolele 12-22 din Regulamentul (UE) 2016/679, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura:
(a) securitatea națională;
(b) apărarea;
(c) securitatea publică;

(d) prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;
(e) alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale;
(f) protejarea independenței judiciare și a procedurilor judiciare;
(g) prevenirea, investigarea, depistarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate;
(h) funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale în cazurile menționate la literele (a)-(e) și (g);
(i) protecția persoanei vizate sau a drepturilor și libertăților altora;
(j) punerea în aplicare a pretențiilor de drept civil.

De asemenea, amânarea, restricționarea, omiterea sau limitarea furnizării de informaţii la cererea persoanei vizate sunt prevăzute la art. 15 și 17 din Legea nr. 363/2018.

- amânarea, restricționarea sau omiterea (Art. 15);
- limitarea dreptului de acces (Art. 17).

Conform art. 20 din Legea nr. 363/2018, în situațiile prevăzute la art. 15, art. 17 alin. (3) sau art. 19 alin. (6) din Legea nr. 363/2018, persoana vizată se poate adresa autorității de supraveghere pentru exercitarea drepturilor prevăzute de lege.

Operatorul are obligația de a informa persoana vizată cu privire la posibilitatea prevăzută la art. 20, alin. (1) din Legea nr. 363/2018.

În situația prevăzută la art. 20, alin. (1) din Legea nr. 363/2018, autoritatea de supraveghere întreprinde măsurile necesare potrivit atribuțiilor sale legale. Autoritatea de supraveghere informează persoana vizată cu privire la aspectele constatate, precum și cu privire la posibilitatea de a se adresa instanței de judecată.

6. AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL (A.N.S.P.D.C.P.)

Potrivit legii de înfiinţare, organizare şi funcţionare (Legea nr. 102/2005), Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (A.N.S.P.D.C.P.) este autoritatea publică cu personalitate juridică, autonomă şi independentă faţă de orice altă autoritate a administrației publice, ca şi faţă de orice persoană fizică sau juridică din domeniul privat.

Autoritatea are ca principal obiectiv apărarea drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în special a dreptului la viaţă intimă, familială şi privată în legătură cu prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. Acest drept are un conţinut complex, de mare importanţă pentru libertatea şi personalitatea cetăţeanului, iar în ţara noastră este garantat prin Constituţie (art. 26).

Legalitatea prelucrărilor de date cu caracter personal care cad sub incidenţa Regulamentului (UE) 2016/679 și a legislației de transpunere a Directivei (UE) 2016/680 este monitorizată şi controlată de Autoritatea de supraveghere.

În acest scop autoritatea de supraveghere are următoarele sarcini (art. 57 din Regulament):

- monitorizează şi asigură aplicarea regulamentului;

- promovează acţiuni de sensibilizare şi de înţelegere în rândul publicului a riscurilor, normelor, garanţiilor şi drepturilor în materie de prelucrare. Se acordă atenţie specială activităţilor care se adresează în mod specific copiilor;
- oferă consiliere, în conformitate cu dreptul intern, parlamentului naţional, guvernului şi altor instituţii şi organisme cu privire la măsurile legislative şi administrative referitoare la protecţia drepturilor şi libertăţilor persoanelor fizice în ceea ce priveşte prelucrarea;
- promovează acţiuni de sensibilizare a operatorilor şi a persoanelor împuternicite de aceştia cu privire la obligaţiile care le revin în temeiul regulamentului;
- la cerere, furnizează informaţii oricărei persoane vizate în legătură cu exercitarea drepturilor sale în conformitate cu regulamentul şi, dacă este cazul, cooperează cu autorităţile de supraveghere din alte state membre în acest scop;
- tratează plângerile depuse de o persoană vizată, un organism, o organizaţie sau o asociaţie în conformitate cu articolul 80 din RGPD şi investighează într-o măsură adecvată obiectul plângerii şi informează reclamantul cu privire la evoluţia şi rezultatul investigaţiei, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigaţii mai amănunţite sau coordonarea cu o altă autoritate de supraveghere;
- cooperează, inclusiv prin schimb de informaţii, cu alte autorităţi de supraveghere şi îşi oferă asistenţă reciprocă pentru a asigura coerenţa aplicării şi respectării regulamentului;
- desfăşoară investigaţii privind aplicarea regulamentului, inclusiv pe baza unor informaţii primite de la o altă autoritate de supraveghere sau de la o altă autoritate publică;
- monitorizează evoluţiile relevante, în măsura în care acestea au impact asupra protecţiei datelor cu caracter personal, în special evoluţia tehnologiilor informaţiei şi comunicaţiilor şi a practicilor comerciale;
- adoptă clauze contractuale standard menţionate la articolul 28 alineatul (8) şi la articolul 46 alineatul (2) litera (d) din regulament;
- întocmeşte şi menţine la zi o listă în legătură cu cerinţa privind evaluarea impactului asupra protecţiei datelor, în conformitate cu articolul 35 alineatul (4) din regulament;
- oferă consiliere cu privire la operaţiunile de prelucrare menţionate la articolul 36 alineatul (2) din regulament;
- încurajează elaborarea de coduri de conduită în conformitate cu articolul 40 alineatul (1), îşi dă avizul cu privire la acestea şi le aprobă pe cele care oferă suficiente garanţii, în conformitate cu articolul 40 alineatul (5) din regulament;
- încurajează stabilirea unor mecanisme de certificare, precum şi a unor sigilii şi mărci în domeniul protecţiei datelor în conformitate cu articolul 42 alineatul (1) şi aprobă criteriile de certificare în conformitate cu articolul 42 alineatul (5) din regulament;
- acolo unde este cazul, efectuează o revizuire periodică a certificărilor acordate, în conformitate cu articolul 42 alineatul (7) din regulament;
- elaborează şi publică criteriile de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu articolul 41 şi a unui organism de certificare în conformitate cu articolul 43 din regulament;
- coordonează procedura de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu articolul 41 şi a unui organism de certificare în conformitate cu articolul 43 din regulament;
- autorizează clauzele şi dispoziţiile contractuale menţionate la articolul 46 alineatul (3) din regulament;
- aprobă regulile corporatiste obligatorii în conformitate cu articolul 47 din regulament;
- contribuie la activităţile comitetului;
- menţine la zi evidenţe interne privind încălcările prezentului regulament şi măsurile luate, în special avertismentele emise şi sancţiunile impuse în conformitate cu articolul 58 alineatul (2) din regulament;
- îndeplineşte orice alte sarcini legate de protecţia datelor cu caracter personal.

A.N.S.P.D.C.P. facilitează depunerea plângerilor menţionate la art. 57, alin. (1), lit. (f) din RGPD prin măsuri precum punerea la dispoziţie a unui formular de depunere a plângerii care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.

Îndeplinirea sarcinilor autorităţii de supraveghere este gratuită pentru persoana vizată. În cazul în care cererile sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, autoritatea de supraveghere poate percepe o taxă rezonabilă, bazată pe costurile administrative, sau poate refuza să le trateze.

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 îşi are reşedinţa obişnuită, 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.

În vederea apărării drepturilor prevăzute de Regulamentul (UE) 2016/679 și/sau de Legea nr. 363/2018, persoanele ale căror date cu caracter personal fac obiectul unei prelucrări efectuate în cadrul I.G.P.F., pot înainta plângere către A.N.S.P.D.C.P. la sediul acesteia din B-dul G-ral Gheorghe Magheru nr. 28-30, sector 1, Bucuresti, cod 010336, fax: 031.805.96.02, Internet: **www.dataprotection.ro,** sau e-mail: **anspdcp@dataprotection.ro.**
Pentru a depune o plângere la A.N.S.P.D.C.P. click aici

Pe durata tuturor prelucrărilor de date personale, I.G.P.F. se supune controlului Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (http://www.dataprotection.ro) și dezvoltă relații de colaborare cu Oficiul Responsabilului cu Protecția Datelor Personale din cadrul Ministerului Afacerilor Interne, care este structura specializată care exercită îndrumarea, coordonarea și monitorizarea aplicării unitare a legislației în domeniul protecției persoanelor cu privire la prelucrarea datelor cu caracter personal de către structurile și unitățile Ministerului Afacerilor Interne.

De asemenea, sunt avute în vedere ghidurile, deciziile și recomandările emise de către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și documentele de coordonare elaborate de Oficiul Responsabilului cu Protecția Datelor Personale din cadrul Ministerului Afacerilor Interne:

- Legea nr. 102 din 3 mai 2005 *privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată, cu modificările și completările ulterioare*;
- Legea nr. 129 din 15.06.2018 *pentru modificarea şi completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;*
- Decizia ANSPDCP nr. 128/2018 *privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE*;
- Decizia ANSPDCP nr. 133 din 3 iulie 2018 *privind aprobarea Procedurii de primire și soluționare a plângerilor*;
- Decizia ANSPDCP nr. 161 din 9 Octombrie 2018 *privind aprobarea Procedurii de efectuare a investigațiilor*;

- Decizia ANSPDCP nr. 238 din 18 decembrie 2019 *privind modificarea anexei nr. 2 la Procedura de efectuare a investigaţiilor*;
- Decizia ANSPDCP nr. 174 din 18 octombrie 2018 *privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal*;

Link-uri utile:

- https://www.dataprotection.ro/
- https://www.edpb.europa.eu/edpb_ro
- https://www.edps.europa.eu/_en
- https://commission.europa.eu/law/law-topic/data-protection_ro
- https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

7. DEFINIȚII

Date cu caracter personal - *orice informaţii privind o persoană fizică identificată sau identificabilă (persoana vizată); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;*

Prelucrare – *orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;*

Operator - *persoană fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;*

Persoana împuternicită de operator - *persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;*

Autoritate de supraveghere - *o autoritate publică independentă instituită de un stat membru în temeiul art. 51 din Regulamentul nr. 679/2016;*

Autoritate de supraveghere vizată - *o autoritate de supraveghere care este vizată de procesul de prelucrare a datelor cu caracter personal deoarece:*

- *operatorul sau persoana împuternicită de operator este stabilită pe teritoriul statului membru al autorității de supraveghere respective;*
- *persoanele vizate care îşi au reşedinţa în statul membru în care se află autoritatea de supraveghere respectivă sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare;*
- *la autoritatea de supraveghere respectivă a fost depusă o plângere.*

Încălcarea securității datelor cu caracter personal – *înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;*

Sistem de evidenţă a datelor cu caracter personal – *orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice*.

8. PRINCIPII ŞI LEGALITATEA PRELUCRĂRII DATELOR CU CARACTER PERSONAL

8.1. Principii legate de prelucrarea datelor cu caracter personal:

Conform art. 5 din Regulamentul general privind protecția datelor, datele sunt:

- prelucrate în mod legal, echitabil şi transparent faţă de persoana vizată (*„legalitate, echitate şi transparenţă”*);
- colectate în scopuri determinate, explicite şi legitime şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile iniţiale *(„limitări legate de scop”*); adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate *(„reducerea la minimum a datelor”*);
- exacte şi, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt şterse sau rectificate fără întârziere *(„exactitate”*);
- păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele;
- datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, sub rezerva punerii în aplicare a măsurilor de ordin tehnic şi organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor şi libertăţilor persoanei vizate *(„limitări legate de stocare”*);
- prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („*integritate şi confidenţialitate*”).

8.2. Legalitatea prelucrării:

Conform art. 6 din Regulamentul general privind protecția datelor, prelucrarea este legală numai dacă şi în măsura în care se aplică cel puţin una dintre următoarele condiţii:

a) persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
c) prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale care îi revine operatorului;
d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
e) prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul;
f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terţă, cu excepţia cazului în care prevalează interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

9. DATE DE CONTACT

INSPECTORATUL GENERAL AL POLIȚIEI DE FRONTIERĂ (I.G.P.F.)

Sediul: București, sector 6, Bulevardul Geniului, nr. 42C
Adresa e-mail: pfr@igpf.ro;
Telefon: 021.316.25.98; 021.318.25.92;
Fax: 021.312.11.89;
Telefon de informare: (+4)0219590.

RESPONSABILUL CU PROTECȚIA DATELOR CU CARACTER PERSONAL

La nivelul I.G.P.F. funcţionează Compartimentul Protecția Datelor cu Caracter Personal;
Sediul: București, sector 6, Bulevardul Geniului, nr. 42C;
Adresa e-mail: dataprotection.igpf@igpf.ro / sergiu.malita@igpf.ro;
Telefon: 021.316.25.98/ interior 19.270, fax 021.316.35.11.

AUTORITATEA NAŢIONALĂ 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;
Adresa e-mail: anspdcp@dataprotection.ro.
Pentru a depune o plângere la A.N.S.P.D.C.P. click aici

INSPECTORATUL TERITORIAL AL POLIȚIEI DE FRONTIERĂ SIGHETU MARMAȚIEI

Sediul: Sighetu Marmației, strada Dragoș Vodă, nr. 38, cod 435500, jud. Maramureș
Adresa e-mail: itpf.sighetu.marmariei@mai.gov.ro;
Telefon: 0262 314 528;
Fax: 0262 316 446.

INSPECTORATUL TERITORIAL AL POLIȚIEI DE FRONTIERĂ ORADEA

Sediul: Oradea, strada Calea Aradului, nr. 2, cod 410223, jud. Bihor
Adresa e-mail: ijpf.bihor@mai.gov.ro;
Telefon: 0259 401 400;
Fax: 0259 418 924.

INSPECTORATUL TERITORIAL AL POLIȚIEI DE FRONTIERĂ TIMIȘOARA

Sediul: Timișoara, strada Sever Bocu, nr. 49, cod 300278, jud. Timiș
Adresa e-mail: itpf.timisoara@mai.gov.ro;
Telefon: 0257 306 340;
Fax: 0256 306 355.

INSPECTORATUL TERITORIAL AL POLIȚIEI DE FRONTIERĂ GIURGIU

Sediul: Giurgiu, strada Mircea cel Bătrân, nr. 36, cod 080036, jud. Giurgiu
Adresa e-mail: itpf.giurgiu@mai.gov.ro;
Telefon: 0246 213 640;
Fax: 0246 211 785.

INSPECTORATUL TERITORIAL AL POLIȚIEI DE FRONTIERĂ IAȘI

Sediul: Iași, strada George Coșbuc, nr. 3-5, cod 700469, jud. Iași
Adresa e-mail: itpf.iasi@mai.gov.ro;
Telefon: 0232 272 220;
Fax: 0232 460 094.

Garda de Coastă Constanța
Sediul: Constanța, Aleea Zmeurei, nr. 3, cod 900433, jud. Constanța
Adresa e-mail: gardadecoasta.igpf@mai.gov.ro;
Telefon: 0241 641 188;
Fax: 0241 698 668.

Ministerul Afacerilor Externe - Centrul Național de Vize
Sediul: Aleea Alexandru nr. 31, sector 1, București, cod poștal 011822
Tel: +40214311100; +40 21 431 15 62; +40 21 319 21 08; +40 21 319 21 25
Fax: +40 21 319 68 62
Email: dpo@mae.ro

Potrivit art. 44 din Legea nr. 271/2010, cererile care privesc exercitarea drepturilor persoanei vizate în contextul prelucrării datelor cu caracter personal în Sistemul National de Informaţii privind Vize (SNIV) sau Sistemul de Informaţii privind Vizele (VIS) se adresează Centrului National de Vize, iar răspunsul va fi comunicat petentului cât mai curând posibil, dar nu mai târziu de 60 de zile de la data primirii cererii.

Această secțiune a fost a fost actualizată la data de 16.07.2025.